USER PRIVACY OR CYBER SOVEREIGNTY?
Assessing the human rights implications of data localization
TABLE OF CONTENTS

1. Introduction ................................................................................................................. 1
2. Background on data regulation .................................................................................. 2
3. Methodology for assessment ...................................................................................... 4
4. Human rights implications ........................................................................................... 5
5. Global landscape ........................................................................................................ 7
6. Conclusion .................................................................................................................. 13
7. Appendix:
   Framework for assessing human rights implications of data localization requirements .............................................. 14

Acknowledgements

Adrian Shahbaz is director for technology and democracy at Freedom House. Allie Funk is senior research analyst. Andrea Hackl is an independent consultant. The authors are grateful to Noah Buyon, Cathryn Grothe, Amy Slipowitz, and Kian Vesteinsson for assistance in the research and writing of the report.

This report was produced with support from Facebook. It draws on data from Freedom on the Net, Freedom House’s flagship report on human rights online, which is supported by the U.S. State Department’s Bureau of Democracy, Human Rights and Labor (DRL), the New York Community Trust, and Internet Society.

Find this report online at:
1. Introduction

Amid declining faith in the international system, a different form of protectionism is gaining steam with adverse consequences for billions of internet users. Authorities in a growing number of countries are weighing measures to control the flow of data in and out of their national borders. Cyber norms promoted by China and Russia are expanding to countries such as Brazil, India, and Turkey, where legislators had been debating data localization provisions as this report went to press. If passed, these measures will facilitate the collection of sensitive data by government agencies, enabling a further crackdown on free expression, privacy, and a range of human rights. This splintering of the internet will also embolden more governments to pursue a model of cyber sovereignty, with grave implications for the future of internet freedom.

This report examines the implications of data localization policies on users’ human rights. It begins by providing background on data regulation, including the various types of electronic data as well as how terms like “data localization,” “data protection,” and “data privacy” are commonly used. The report then outlines a robust framework for evaluating the impact of data localization laws on human rights, before launching into an analysis on legislation that has been passed or proposed in eight different countries. Understanding a law’s political and internet freedom context is vital for evaluating its human rights impact on members of civil society, marginalized communities, and the general population. The report concludes with an analysis of what this alarming trend means for the future of the free, open, and global internet.

Data localization typically has not received the same level of attention as other internet freedom issues, such as encryption, disinformation, social media blocking, and network shutdowns. Yet the privacy of our personal data is fundamental to the protection of our human rights. The information that is generated and gathered through the casual use of online services reveals a great deal about our personal and professional lives. Geolocation data can provide insight into a user’s participation in a peaceful protest, the frequenting of a religious establishment, or membership in a social movement. Inferences drawn from our browsing activity and “Likes” can reveal sensitive information such as our sexual orientation and health status. Data localization grants officials access to a massive dataset in their drive to root out those who deviate from religious doctrine, violate local laws on “insulting” public officials, or pose a “threat” to public order by virtue of their autonomous existence. This can lead not only to flagrant abuses against particular individuals, but also a crackdown on democratization movements more broadly.

Proponents of these data localization provisions often cite the need to protect national security, promote the local digital economy, or safeguard the privacy of users. Real and perceived failures of the existing internet governance system have motivated governments across the democratic spectrum to impose their own rules and checkpoints on cross-border data flows. However, the strengthening of state control over users’ data does little to address genuine grievances surrounding cybersecurity,
disinformation, or the online targeting of marginalized communities by state and nonstate actors. National security interests often co-opt arguments for greater data privacy to justify an expansion of censorship and surveillance powers. Indeed, the rise in data localization policies has been a contributing factor in declining internet freedom.

Strong data privacy legislation is important for carving out protections against government surveillance and corporate malfeasance. These laws should be focused on respecting users’ privacy, rather than simply increasing government power over the private sector. Better collaboration between policymakers, technology companies, and civil society may also prove effective. After all, some of the most important advances in privacy—such as the widespread adoption of end-to-end encryption or HTTPS browsing—derive from innovations in technical standards and product design. Ultimately, multistakeholder efforts will be needed to ensure leading democracies can offer a viable alternative to the authoritarian model of cyber sovereignty.

2. Background on data regulation

Especially over the last decade, governments around the world have adopted data localization requirements to regain control over global data flows. The stated rationale behind these requirements vary from attempts to secure users’ data from foreign governments, the protection of national security interests, the economic incentives around building local data centers or reducing competition from foreign companies, increasing law enforcement access to data, enforcing local censorship laws, and undermining encryption. Particularly in repressive information environments, unconstrained and centralized access to user data can lead to serious human rights harms.

**Personal data**

This report examines the human rights implications of forced localization of personal data. Legal frameworks generally consider personal data to be data that identify a person, such as a name or a biometric identifier, or data that could be analyzed to identify a person, like a home address, an IP address, or a person’s appearance. The EU’s General Data Protection Regulation (GDPR), for example, defines personal data as “any information relating to an identified or identifiable natural person.” The regulation excludes data with no relation to a person and no potential to identify a person (that is, properly anonymized data), and data relating to a person who has died. A subset of especially sensitive data, labeled special categories of personal data—such as data revealing racial or ethnic origin, information about a person’s sex life or sexual orientation, and biometric data used for identification—receive special safeguards.

Categorizing a subset of personal data as especially sensitive is modeled in proposed and implemented data protection laws in several countries, including Turkey, India, Japan, the Philippines, and South Africa. Other laws do not offer special protections to a subset of personal data, as in Hong Kong, or broaden the definition of personal data, as with the U.S. state of California’s data protection law, which also protects data relating to households.

Despite the name a bill may take, data protection and localization are distinct policy areas. Some data protection regulations may also contain rules related to data localization. For example, Turkey’s Law on the Protection of Personal Data lays out additional requirements regarding the cross-border transfer of sensitive personal data. Sensitive personal data includes information related to race and ethnicity, political opinion, and biometric data. Turkish law has additional processing restrictions for information related to health and sexual life. Data storage requirements included in Pakistan’s Citizens Protection (Against Online Harm) Rules broadly require social networking services to store “data and online content.” The Rules go into more detail regarding the types of information that may be handed over to authorities, which may include “subscriber information, traffic data, content data and any other information or data.”
Data localization

Data localization refers to rules governing the storage and transfer of electronics data across a national jurisdiction. These requirements can take many different forms. For example, a government may require all companies collecting and processing certain types of data about local users to store the data on servers located in the country. Authorities may also restrict the foreign transfer of certain types of data or allow it only under narrow circumstances, such as after obtaining the explicit consent of users, receiving a license or permit from a public authority, or conducting a privacy assessment of the country to which the data will be transferred.

Moreover, localization requirements may refer only to certain types of data. For example, in Germany, a law that took effect in July 2017 requires domestic storage of telecommunications metadata such as location data and IP addresses. The Australian government requires health records to be stored within the country. A proposal in India would require the local storage of sensitive personal data (including, for example, health information and religious beliefs) and critical personal data (information related to national security and other related matters as defined by the central government). Similarly, Article 37 of China’s Cybersecurity Law broadly refers to personal information and important data to be stored within the country’s borders. According to the law’s definition of personal information, this information refers to data that could by itself or combined with other information could identify a person. This could include a wide range of information, including a user’s full name, phone number, or address.

Data protection

It is important to note that strong data protection measures do not require the forced localization of information within a specific territory or jurisdiction. Perhaps the best example of this is the GDPR, which came into effect in May 2018 and remains the most comprehensive data protection framework in the world. Under article 45 of the GDPR, international data transfers of personal data can take place only if the receiving country has adequate protections in place. In determining adequacy levels for receiving countries, the commission takes into consideration a variety of factors such as a country’s respect for the rule of law and human rights as well as national security and criminal laws. In January 2019, the European Union issued its first adequacy decision, allowing the transfer of personal data between countries of the European Economic Area (EEA) and Japan.

Since 2016, the EU-US Privacy Shield framework has governed data transfers to the US, permitting transfers where entities had committed to certain privacy standards modeled after the pre-GDPR EU data directive. However, in July 2020 the European Court of Justice (ECJ) invalidated Privacy Shield on the basis that U.S. national security surveillance programs limit the protection of any personal data transferred to the U.S. Cross-border data transfers can continue under agreements known as standard contractual clauses, binding rules for data transfers to third countries approved by a member state’s Data Protection Authority, though the court now requires stricter scrutiny of third country surveillance laws. Data flows that are voluntary or “necessary” under the GDPR are not limited by the ECJ ruling.

The ECJ ruled Privacy Shield invalid in part because the court found that U.S. national security surveillance programs fail to meet the principles of necessity and proportionality in restricting the rights of European Union citizens, as required under the EU Charter of Fundamental Rights. The GDPR permits member states and the European Union to derogate data rights in the context of necessary and proportionate measures to protect national security or public security, among other reasons. A country derogating from the GDPR must provide safeguards against abuse, data retention limits, an impact assessment, and other protections for the rights and freedoms of EU citizens. Importantly, the ECJ did not address laws passed by member states such as France and Germany, which have derogated data rights in the name of national security, facilitating the operation of sophisticated telecommunications surveillance programs. The ruling raises questions on whether leading democracies can successfully promote a viable alternative to the authoritarian model of cyber sovereignty. For policymakers in the U.S., it also highlights how preserving a free, open, and global internet requires greater effort to ensure strong protections for human rights at home.
Data privacy

Although at times used interchangeably, data privacy offers a more robust framework than data protection. Data protection laws often only regulate the lawful access and use of data collected and stored by private companies. Data privacy laws go further in their protections by granting users’ control over their personal information, including by clarifying how data is collected and stored; which government agencies, private companies, or other third parties can access it and the process for doing so; and for what purposes state and nonstate actors can use that information. Given this more comprehensive approach, data privacy laws are more effective in safeguarding fundamental freedoms.

3. Methodology for assessment

Data localization requirements do not operate in a vacuum. Rather, a country’s political context, international relations, and economic imperatives all have a role to play in shaping a government’s approach to governing data flows. Another critical factor, and sometimes even a motivating factor, is a country’s approach toward human rights and the role that the internet can play in either facilitating or restricting privacy, freedom of expression, and other fundamental rights in a global context. Particularly in authoritarian regimes like China and Russia that have long pursued a sovereign digital agenda, data localization requirements have become another tool to further erode human rights.

Data localization requirements have also emerged in democracies, raising questions of whether and how human rights concerns resulting from these requirements differ across different political contexts. Based on our review of data localization requirements, we propose a three-layered framework that could help policymakers, companies, and civil society to assess the human rights risks that could result from the forced localization of data. Broadly, these factors can be evaluated based on three interdependent assessment levels:

- **Scope of data localization requirement:** An analysis of the human rights impact of new legislation should begin with a thorough review of the enacted or proposed regulation. What are the types of data that need to be stored within a country? What are the specific rules around collection and processing of data? Are data processors required to conduct a privacy impact assessment of the receiving country, and do they have to obtain a security permit from authorities before data can be transferred to a different country? What are some other factors that define the data localization law?

- **Governance landscape:** Evaluations should also take note of the larger context in which a data localization requirement was proposed and enacted. Have rules been drafted in consultation with relevant stakeholders (business, technical experts, human rights advocates, civil society groups representing vulnerable communities, etc.)? Have they been opened up for public consultation? Will they be passed by a representative body elected through free and fair elections? If passed, will they subject to constitutional review from an independent court?

- **Human rights landscape:** On a fundamental level, it is critical to evaluate whether a government respects rule of law and due process, as well as the level of judicial independence in a country. For example, the risks to users’ privacy and other human rights are particularly high if authorities are able to engage in unlawful surveillance and censorship that does not comply with international human rights standards. For a full set of questions, please see “Appendix: Framework for assessing human rights implications of data localization requirements.”
4. Human rights implications

Data privacy is essential to the protection and enjoyment of human rights. Domestic data storage requirements place users’ data firmly in the legal purview of governments, significantly enhancing authorities’ surveillance capabilities by lowering access barriers to this data. Law enforcement agencies regularly examine electronics data to gather evidence of an individuals’ alleged wrongdoing. In many cases, surveillance agencies continuously monitor online platforms for behavior that may violate local laws. In others, authorities begin with a particular target in mind, later enlisting data analysis tools to sift through large amounts of personal information in order to find a data point that can be exploited to justify an accusation. Security agencies use these methods both for purposes that may be deemed necessary and proportionate under international human rights standards, as well as for conducting clear violations of human rights.

Privacy

Grounding many of the human rights implications of data localization is the fundamental right to privacy as guaranteed in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). In our digital lives, we create and leave behind traces of data that can reveal much about our personal lives. A user’s geolocation data can reveal if they frequented a peaceful protest or place of worship. Insight into a user’s list of contacts or networks can expose whether they associate with friends of particular political affiliations. And data from credit card purchases can reveal a user’s sexual orientation. The ubiquitous collection, storage, and processing of data is an affront to privacy, particularly without adequate safeguards around data protection.

Freedom of expression

Requirements to store information such as users’ social media posts, private messages, and online articles on local servers may threaten the right to free expression as guaranteed by Article 19 of the ICCPR. The annual Freedom on the Net report found that a record number of governments prosecuted users for nonviolent political, social, and religious posts in 2019, signaling a greater willingness and capacity to target individuals for their online expression. An increase in data localization would likely exacerbate this trend by providing authorities with a more extensive dataset of the populations’ written opinions.

Freedom House research has demonstrated how security agencies parse through the social media posts of well-known activists and regime opponents in order to find material that could be used to launch a prosecution. Authorities often rely on vague laws related to defaming public officials, harming foreign relations, spreading false information, harming national security, destabilizing public order, encouraging extremism, or insulting religious feelings to target legitimate online expression.

Access to information

Data localization requirements are often part of a wider bid to enforce online censorship, denying users’ right to access to information as guaranteed under Article 19 of the ICCPR. Governments have blocked access to social media platforms and messaging apps over failures to adhere to localization provisions. Technology companies and media outlets are aware that the storage of information on local servers could open up for new avenues for the government to issue takedown orders for journalism, discussion of human rights, educations materials, or political, social, cultural, religious, and artistic expression deemed to contravene the country’s laws. Even the threat of data localization has been used to push companies large and small to remove content that could be deemed illegal in a process that lacks judicial oversight and standard protections for necessity, proportionality, transparency, and redress.
Press freedom

Freedom of the press is critical to hold those in power to account, to draw attention to human rights abuses and injustices, and to ensure a functioning democracy. Press freedom is protected under Article 19 of the ICCPR, but can be threatened by requirements on media companies to host their websites and store sensitive information on local servers. Data localization laws may be used to force news outlets to obtain a government license and comply with censorship orders. They also threaten the privacy and security of journalistic sources, particularly when combined with measures to outlaw or undermine encryption.

Freedom of belief

Freedom of religion and belief is a protected human right under Article 18 of the ICCPR. Article 27 further protects the rights of religious minorities in a country to exercise their own religion. However, religious minorities continue to be subject to human rights abuses in countries around the world. In China’s abuses against Uighur Muslims in Xinjiang, social media histories have been used as evidence to detain and arrest Uighurs due to alleged religious offenses. Under China’s stringent data localization regime, personal data such as names and addresses are readily available to Chinese authorities, exacerbating persecution and human rights abuses against Uighurs and other minority communities.

Nondiscrimination and equal rights

Restrictions on data storage and transfer also undermine equal application of human rights standards and protection against discrimination, as stated in Articles 2 and 26 of the ICCPR. Data localization can make it easier for governments to identify and persecute individuals belonging to certain distinct groups, including ethnic, religious, gender, LGBTQ, and other relevant communities. These risks can be compounded by systemic racism, discriminatory laws, or a broader environment of impunity for human rights abuses against at-risk populations. For example, data localization requirements exacerbate the human rights risks posed by Russia’s law banning the dissemination of information on “nontraditional sexual relationships.”

Freedom of assembly

The right to peaceful assembly, as guaranteed by Article 21 of the ICCPR, is vital for awareness-raising, community organizing, and holding powerful state and nonstate actors accountable for corruption, misconduct, and human rights abuses. Social media platforms have become essential tools for activist organizing, and data localization laws make it easier for authorities to identify and monitor protestors by surveilling their online activity and gaining easy access to their personal information. Knowing that the government has yet another legal tool to access personal information, people may also be deterred from participating in protests.

Freedom of association

Insofar as they may weaken privacy, data localization also threatens individuals’ right to join groups and participate in civic engagement as outlined in Article 22 of the ICCPR. In countries where women face barriers to reporting sexual harassment and unfair working conditions, for example, participating in advocacy groups and voluntary associations can provide critical fora to address unequal treatment and harassment. Labor unions help workers fight for stronger protections, equal pay, and fair working conditions. These nongovernmental organizations play a fundamental role in promoting and protecting human rights, as well as providing a people-powered check against the activities of the government. However, knowledge that one’s professional and civic associations can be readily viewed by law enforcement has a chilling effect on these important activities.

Due process

Respect for due process and the right to a fair trial as guaranteed by Article 14 of the ICCPR underpins the protection of human rights, ensures that government institutions and processes are not at the whim of politics or a security agency, and allows people...
to hold state and private actors accountable for wrongdoing. Particularly in countries with disregard for due process, data localization requirements open the door for arbitrary, disproportionate, and discriminatory surveillance. By requiring localized data storage, a country with weak judicial independence and a poor track record on human rights could bypass the procedures to request data stored in countries with strong rule of law, often codified in a mutual legal assistance treaty (MLAT) with a warrant requirement. In countries with low levels of judicial independence, authorities may be able to obtain a warrant that is rubber-stamped by a judge to create the illusion of due process. In more egregious cases, storing data within the geographic reach of state authorities could make it easy for them to visit a data center and pressure an employee to hand over user data without following human rights standards for due process.

**Personal security**

Article 9 of the ICCPR protects people’s fundamental right to personal security. However, the lives of dissidents, human rights activists, and other opposing voices continue to be under threat around the world. Ready access to data sought by law enforcement and authorities poses grave risks to human rights. In some cases, users may even face threats to their lives if there is little constraint on government access to information. In Pakistan, users have been sentenced to death for social media posts deemed blasphemous by the government, although the cases remain on appeal.\(^3\) If implemented, Pakistan’s Citizens Protection (Against Online Harm) Rules would require social media companies to establish domestic data servers and hand over a wide range of user information, including content. These requirements would make it even easier for the government to identify and track down users accused of blasphemy or other illegal activities.\(^3\)

5. **Global landscape**

Data localization provisions are implemented within a variety of political contexts and their scope can differ significantly, particularly as it relates to the types of data under scrutiny. Below is a non-exhaustive but indicative list of countries that have proposed or passed localization requirements pertaining to personal data, as well as an overview of the human rights context and implications in each country. Most concerning are the stringent requirements found in countries ranked as “Not Free” or “Partly Free” according to *Freedom on the Net*,\(^4\) where data localization provisions are often introduced as part of a wider crackdown on internet freedom.

![China – Not Free](https://www.freedomhouse.org)

Over the last decade, Chinese users’ ability to exercise their human rights online has rapidly declined, making China the most repressive information environment in the world.\(^5\) An increasingly sophisticated surveillance and censorship machinery, citizens’ arrest for online activities, and targeted network shutdowns have allowed the government to tighten its grip around an already restrictive online environment. Domestic data storage requirements and restrictions of cross-data transfers under China’s Cybersecurity Law exacerbate the weak protections for human rights in the country.

China’s Cybersecurity Law went into effect in June 2017, and has further eroded the nominal privacy protections that were left in the country. Many provisions contained in the law have significantly bolstered China’s comprehensive surveillance apparatus, including forced data localization, real name registration requirements, and mandates for network operators to assist police and security agencies with criminal investigations or national security operations.\(^6\) Separately, the Chinese government has introduced several policies requiring real name registration and providing authorities with broad powers to enter the premises...
of internet service companies, ensuring that users can be easily identified and that their data can be inspected and copied when deemed important to cybersecurity.¹⁷

Data localization requirements under the country’s Cybersecurity Law apply to a broad set of companies and data, replacing a piecemeal framework that covered different sectors such as e-banking and health information.³⁸ According to Article 37 of the law, operators of “critical information infrastructure” are required to store personal data, as well as data deemed “important” (for example, data related to national security and public interest), within the country's borders. All cross-border data transfers of this data require a security assessment. The government continues to release standards and measures that define and operationalize the Cybersecurity Law.³⁹ After the law was passed, Apple, for example, quickly complied with the requirement, announcing plans that year to open a data center in China.⁴¹ In February 2018, Apple’s iCloud began storing the data of its Chinese users in partnership with the state-run company Guizhou-Cloud Big Data.⁴¹

Chinese President Xi Jinping speaks by video conference to delegates at the opening ceremony of the World Internet Conference in Wuzhen, China’s Zhejiang province on November 16, 2016. Photo credit: STR/AFP via Getty Images.

### Vietnam – Not Free

The Vietnamese government has long sought to impose authoritarian-style control over the internet. Data localization requirements, most recently through the Cybersecurity Law, are one of the myriad ways in which service providers and technology companies are required to aid the government in monitoring the communications of their users. This draconian surveillance environment is coupled with routine years-long convictions of activists and journalists for their online speech, as well as systematic content manipulation. Alarmingly, the ruling party has increasingly fixated itself on scrubbing any trace of critical or “toxic” speech online.

Introduced in 2018 and entering into force in January 2019, the Cybersecurity Law dramatically increased data retention and localization provisions. A draft decree guiding the law’s implementation would have seemingly required online platforms—including large entities such as Facebook and Google, as well as smaller platforms such as payment services and game companies—to store data on Vietnamese users locally and to provide that data to the government upon request.⁴² Data, including names, birth dates, nationality, identity cards, credit card numbers, biometrics files, and health records, had to be stored for as long as a service operates within Vietnam. Additionally, content of communications and contact lists would also
be stored for 36 months. Foreign companies that serve over 10,000 local customers would also be required to have offices in Vietnam.43

However, in the fall of 2019, the government reportedly released a revised draft decree that narrowed data localization requirements, only triggering them when certain companies do not abide by Vietnamese law, which includes vague provisions criminalizing online speech and imposing intermediary liability.44 Companies impacted by the requirements include those which provide services on the internet, telecommunications networks, or otherwise cyberspace.

The 2013 Decree 72 on the Management, Provision, Use of Internet Services and Internet Content Online also mandates that companies maintain at least one domestic server “serving the inspection, storage, and provision of information at the request of competent authorities,” and requires them to store certain data for a specified period. It also requires providers such as social networks to “provide personal information of the users related to terrorism, crimes, and violations of law” to “competent authorities” on request, but lacks any meaningful oversight to discourage abuse.

Since 2019, the Cybersecurity Law and its associated data localization provisions have seemingly created an environment in which online platforms have had to capitulate with content removal demands, threatening the already shrinking space where Vietnamese users can exercise their rights to free expression, access to information, and other fundamental freedoms. Google has been praised by the Minister of the Ministry of Information and Communications (MIC) for being “collaborative.” The company, for example, was said to have removed over 7,000 video and 19 YouTube channels of “malicious, illegal” content as of May 2019.45 Similarly, in August 2019, the MIC’s Minister announced that Facebook was meeting 70 to 75 percent of the government’s content removal requests, up from a reported 30 percent. Moreover, Reuters reported that in February 2020, Facebook’s local servers were taken offline, significantly slowing down services across Facebook, Instagram, and WhatsApp for users in Vietnam.46 Access was restored in early April only after the company allegedly agreed to significantly increase the censorship of “anti-state” posts.

Pakistan – Not Free

Pakistan’s government has proposed data localization requirements through two separate draft laws. These proposals come amidst the authorities’ efforts to tighten their grip over the online space and personal data. The government routinely shuts off connectivity and frequently censors political, religious, and social content. Journalists, activists, and ordinary users critical of those in power not only face intimidation campaigns online and off, but arrests and prosecutions for their online speech. Even more disconcerting, users accused of posting blasphemous content about Islam have received death sentences.

Citing an increase in disinformation and the need to regulate social media and communications platforms, the government proposed the Citizens Protection (Against Online Harm) Rules in February 2020. Notified under both the Telecommunication Act of 1996 and the Prevention of Electronic Crimes Act of 2016 (PECA), the Rules would require companies to remove content deemed illegal within 24 hours of being notified of such content by a newly created National Coordinator office.47 In its current form, the draft law also requires social media companies to establish at least one data server in the country and share data upon request, which may include subscriber information, traffic data, content, or “any other information or data.” This information would need to be provided in a decrypted and “readable” form.48 The draft also requires companies to institute a legal presence in the country and a local office with a country-based representative. Companies failing to comply with this law could be fined or blocked.49

The Rules would significantly expand the governments’ ability to surveil users and force companies to hand over their personal information, as well as undermining platforms’ encryption standards.50 Pakistan’s Digital Rights Foundation, among other civil society groups, have highlighted that the law would allow authorities to request sensitive information without following any legal
or judicial process, violating international human rights law and going beyond the scope of existing powers allowed for under PECA and the Telecommunications Act. These significant concerns for user privacy are even more troubling considering that Pakistan currently does not have a data protection law in place, and has a history of intrusive surveillance and monitoring.

Concerningly, a proposed data protection bill that was first introduced in 2017 and opened up for another round of public consultations in 2020 also includes controversial domestic data storage requirements.

Russia – Not Free

Plans to adopt data localization requirements in Russia came amid the Kremlin’s push to “tame” information technology following antigovernment protests organized in part on social media. This experience, reinforcing President Vladimir Putin’s long-standing suspicion of the internet as a Trojan Horse for Western influence, led to the development of a digital agenda that asserts national sovereignty by reproducing national borders online. In this context, national data storage requirements have supplemented tools such as internet blacklists, troll farms, and SORM (a sophisticated mass surveillance apparatus) that have enabled Russia’s pursuit of digital authoritarianism.

In September 2015, Russia enacted one of the most stringent data localization laws in the world. According to Law No. 242-FZ, both foreign and domestic companies processing personal information of Russian citizens have to store this data on servers located in Russia, or else face blocking. For the Russian government, data localization requirements were the logical next step of a protectionist digital agenda ultimately aimed at wailing off the so-called Runet from the international internet. The data localization law was also seen as an opportunity to shore up Russia’s domestic IT sector. The law has already had impacts on the operations of U.S. companies in the country. In November 2016, LinkedIn became the first major platform to be blocked for its failure to comply with data localization requirements. The government raised the stakes for non-compliance with the law by introducing fines of up to 18 million rubles in December 2019. Facebook and Twitter were fined 4 million rubles each for their continued refusal to store the personal information of Russian citizens on domestic servers in early 2020; both platforms have refused to pay and remain unblocked as of July 2020.

In Russia’s already repressive information environment, data localization requirements provide another rationale to censor online voices expressing critical viewpoints.
Turkey – Not Free

In Turkey, the government’s effort to enhance control over social media platforms has included numerous proposed laws restricting cross border data transfers. The latest attempt came amid the COVID-19 pandemic, when the government reexamined data localization requirements as part of a bill addressing the economic impacts of the pandemic. Under these measures, foreign social media companies with more than one million daily visits from users within Turkey would be required to establish a representative in Turkey responsible for addressing authorities’ concerns about content posted on the platform. The draft bill also required companies to store Turkish users’ data on domestic servers. In a country known for its repressive information environment, such requirements would provide authorities with yet another tool to censor, surveil, and track down internet users. While the Turkish government removed amendments controlling social media from the economic relief bill, in July the government introduced legislation forcing companies to establish a legal representative in the country or face five stages of escalating penalties, including fines, an advertising ban, and bandwidth limitations of up to 90 percent.

Domestic data storage requirements can also be found in Turkey’s data privacy framework, which came into effect in April 2016. According to the Law on the Protection of Personal Data, which is modelled after the EU’s 1995 Data Protection Directive, all cross-border transfers of sensitive and non-sensitive personal information require the explicit consent of data subjects, or have to meet other legal grounds. Data may only be transferred without consent to a country with sufficient protections in place. The Personal Data Protection Board determines which countries have adequate standards of protection and approves cross-border transfers to countries that lack such a standard. Turkish officials continue to release documents and regulations operationalizing the law, but the full extent of how these provisions will be used in practice to control the online activities of Turkish citizens is not yet known. Since the Data Protection Directive that served as a model for Turkey’s data protection framework has now been replaced in the EU by the GDPR, legal experts have noted it puts Turkey out of step with the EU framework.

Indonesia – Partly Free

Despite the impressive democratic progress that Indonesia has made since the fall of an authoritarian regime in 1998, internet freedom continues to be restricted. Authorities deploy internet shutdowns and social media blocks, censor large swaths of content deemed “negative,” spread manipulated news and information, and arrest users and journalists for alleged offenses such as hate speech. In this context, the government continues to mandate registration requirements and other regulations over personal data, though the Ministry of Communication and Information Technology (MCIT) recently eased local data storage requirements for private companies.

In 2012, the Indonesian government introduced Regulation No. 82 of 2012 concerning Implementation of Electronic Transactions and Systems, which required all operators of electronic systems providing “public services” to build data centers in the country for purposes related to law enforcement and data sovereignty. According to media reports, the law was never fully enforced as officials planned to revise provisions on domestic data storage requirements. In October 2019, MCIT introduced a revised version of the law, Regulation No. 71 (PP 71/2019), which eases data localization requirements by limiting them to public entities and exempting the banking and finance sectors. Law PP 71/2019 also requires all digital platforms that operate in Indonesia to register their companies before October 2020. As of July 2020, the government is drafting a ministerial regulation on data centers as an extension of PP 71/2019 that will provide further guidance on domestic data center requirements.

Despite the MCIT relaxing data localization requirements, some companies are establishing local infrastructure in order to take advantage of Indonesia’s thriving digital economy. Google, for example, announced in early 2020 that it would establish domestic data centers to meet customer demand for cloud services. Alibaba Cloud has also had a presence in the country since 2018, and Amazon Cloud is planning to follow suit by establishing a presence in Jakarta.
India – Partly Free

In India, a hybrid data localization regime is among some of the measures considered under the country’s draft Data Protection Bill. For several years, privacy has been on the forefront of digital rights debates in the country, with a landmark Supreme Court ruling in 2017 declaring privacy a constitutionally protected right. Despite the ruling, significant government surveillance, such as the national biometric ID scheme Aadhaar and spyware deployed against activists and lawyers, undermine privacy and other human rights for people in India.

While rights advocates have welcomed the government’s plan to adopt national privacy legislation, several provisions within the Data Protection Bill have come under scrutiny. In December 2019, lawmakers shared a revised draft of the bill which would give data subjects greater control over their data and require companies to be more transparent regarding data collection and processing practices. The draft bill defines three categories of data: sensitive personal data, which includes information related to health and sexual orientation; critical personal data deemed important to the government, which could include national security and military data, with the power to define critical personal data delegated to the government once the bill is law; as well as general data. According to the draft legislation, both sensitive and critical personal data must be stored on domestic servers. Critical personal data can only be processed within the country. Sensitive personal data can be transferred out of the country to be processed, but only if data processors obtain explicit consent from users and meet other requirements, or are subject to the same level of protections as Indian law. After processing, such data or a copy must be brought back into the country for storage.

Civil society groups have raised concerns that the 2019 draft bill would provide authorities with overbroad surveillance powers. Alarmingly, clause 35 of the bill allows the central government to exempt state agencies, which could include law enforcement, from compliance, if such an exemption is “necessary and expedient” and “in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, [and] public order.” The exemption clause, coupled with requirements to store and process certain forms of personal data locally, could worsen India’s already sophisticated surveillance environment.

Before proposing more stringent data localization requirements in the draft data protection law, India took a sectoral approach to data localization, with limited transfer restrictions applying to certain types of data in the areas of banking, healthcare, and telecoms. In April 2018, the Reserve Bank of India also issued a directive that all data related to payment systems such as transaction details has to be stored in India.

Brazil – Partly Free

While Brazil’s legislative framework around internet freedom remains relatively strong, users continue to face obstacles when it comes to fully exercising their human rights online. Signed into law in 2014, the Marco Civil da Internet continues to be one of the world’s most comprehensive laws protecting the rights of internet users. However, in recent years defamation and electoral laws have been weaponized by politicians and businesspeople to silence critical voices, and journalists and activists critical of the government routinely face harassment and intimidation. Since the 2018 presidential election, disinformation has continued to permeate social media, and government figures have been accused of leading such manipulation.

The Brazilian government has introduced dozens of bills addressing disinformation online. In addition to a number of other provisions that could infringe on users’ rights to privacy, the so-called “fake news” bill (PL 2630/2020) proposed the creation of data localization requirements. According to Article 24 of the draft bill, social media companies would be required to establish local offices with a legal representative, and maintain a database within the country to store information on Brazilian users. On June 30, 2020, the Senate passed the fast-tracked bill after scrapping the controversial data localization measures. However,
Article 37 of the updated version, which remained under debate in the Chamber of Deputies as of July 20, obliges social media companies to establish a local representative and remote data access capabilities, which experts have called a “pseudo data localization measure.” The Brazilian government had previously contemplated data localization requirements in the Marco Civil da Internet by restricting cross-border data transfers, but they were ultimately removed from the legislation after opposition from civil society.

Other key initiatives that could better protect users’ privacy have remained stalled. In August 2018, former President Michel Temer signed the General Data Protection Act (Bill 53/2018), but the bill has undergone several rounds of congressional revisions after both President Temer and current President Jair Bolsonaro vetoed key provisions, including the establishment of a politically independent data protection authority. Moreover, full implementation continues to be delayed; President Bolsonaro most recently postponed the bill to May 2021 as part of Provisional Measure #959/2020 addressing the COVID-19 crisis. At the same time, civil society has expressed concerns that measures to contain the pandemic undermine Brazilians’ civil liberties. Law 13.979, passed in February 2020, for instance, expands the powers of the Ministry of Health in an effort to slow the virus. However, experts contend that it also enables unfettered data collection without adequate protections.

6. Conclusion

New restrictions on cross-border data transfer and storage have emerged in numerous countries around the world. For authoritarian regimes such as Russia and China, these regulations are key to reasserting sovereignty online. But these types of regulations are also being embraced by democracies that have long promoted the free flow of information and data across borders. Moreover, data localization requirements are no longer only found in cybersecurity and data protection bills, but have also found their way into bills addressing other pressing political and societal issues such as the COVID-19 crisis and election disinformation.

This report also presented a list of questions and criteria that could help inform frameworks for conducting a more robust human rights impact assessment (HRIA) of specific data localization laws. Such an assessment tool could provide a critical resource for technology companies, civil society, policymakers, and other stakeholders to guide decision-making on the human rights implications of specific products and policies in countries with localization requirements.

Renewed interest in data localization poses a heightened risk for users’ privacy and other fundamental rights. This is particularly concerning as some of the most stringent data localization requirements can be found in countries with poor human rights records and restrictive information environments. Particularly in countries ranked “Not Free” and “Partly Free” by Freedom on the Net, data localization requirements have been introduced under the guise of protecting user privacy and national security, or to develop the local digital economy. However, as the examples presented in this report show, these requirements expand authorities’ surveillance capabilities and erode a broad spectrum of human rights.

It is alarming to see Brazil, India, Pakistan, and Turkey recently consider data localization requirements in various pieces of legislation outlined above. These countries may prove to be the “swing states” of internet governance, paving the way for officials in other countries to abandon internet freedom in favor of a “cyber sovereignty” approach favored by the likes of China and Russia. Ultimately, much will depend on the ability of democratic leaders to advance an alternative mission grounded in protecting privacy while preserving an internet that is open and global.
7. Appendix:
Framework for assessing human rights implications of data localization requirements

**Privacy**
- Are website owners, bloggers, or users in general required to register with the government when posting comments or purchasing electronic devices?
- Are users prohibited from using encryption and anonymization services to protect their communications, and are there laws requiring that providers of encryption services turn over decryption keys to the government?
- Are there legal guidelines and independent oversight on the collection, retention, and inspection of surveillance data by state agencies, and if so, do those guidelines adhere to international human rights standards regarding transparency, necessity, and proportionality?
- Do government surveillance measures target or disproportionately affect political dissidents, human rights activists, journalists, or certain ethnic, religious, gender, LGBTQ, and other relevant groups?
- Are companies (e.g. service providers, providers of public access, internet cafes, social media platforms, email providers, device manufacturers) required to collect and retain data about their users for a certain amount of time, or are they required to monitor users and supply information about their digital activities to the government?
- Are government requests for user data from these companies transparent, and do companies have a realistic avenue for appeal, for example via independent courts?

**Freedom of expression**
- Do specific laws—including those related to the media, defamation, cybercrime, cybersecurity, and terrorism—criminalize online expression and activities that are protected under international human rights standards?
- Are individuals subject to civil liability, imprisonment, arbitrary detention, or other legal sanction for publishing, sharing, or accessing material on the internet in contravention with international human rights standards?
- Are penalties for defamation, spreading false information, national security, extremism, blasphemy, insulting state institutions and official, or harming foreign relations applied to online speech and activities normally under international human rights standards?
- Are individuals subject to physical violence—such as murder, assault, torture, or enforced disappearance—as a result of their online activities, including members in certain online communities or because they belong to a certain ethnic, religious, gender, LGBTQ, or other relevant group?

**Access to information**
- Does the state block or filter, or compel service providers to block or filter, internet content featuring journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression?
- Is there blocking of tools that enable users to bypass censorship?
- Are administrative, judicial, or extralegal measures used to order the deletion of content from the internet, either prior to or after its publication?
- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
Press freedom

- Are journalists subject to pressure or surveillance aimed at identifying their sources?
- Are libel, blasphemy, security, fake news, and other restrictive laws used to punish journalists through either onerous fines or imprisonment?
- Are journalists threatened, harassed online, arrested, imprisoned, beaten, or killed by government or nonstate actors for their legitimate journalistic activities, and if such cases occur, are they investigated and prosecuted fairly and expeditiously?

Freedom of belief

- Are members of religious groups, including minority faiths and movements, harassed, fined, arrested, or beaten by the authorities for engaging in their religious practices?
- Is state monitoring of peaceful religious activity so indiscriminate, pervasive, or intrusive that it amounts to harassment or intimidation?
- Are individuals free to eschew religious belief and practices in general?

Nondiscrimination and equal treatment

- Are members of various distinct groups—including ethnic, religious, gender, LGBTQ, and other relevant groups—able to effectively exercise their human rights with full equality before the law?
- Do members of such groups face legal and/or de facto discrimination in areas including employment, education, and housing because of their identification with a particular group?
- Do noncitizens—including migrant workers and noncitizen immigrants—enjoy internationally recognized human rights, including the right not to be subjected to torture or other forms of ill-treatment, the right to due process of law, and the freedoms of association, expression, and religion?

Freedom of assembly

- Are peaceful protests, particularly those of a political nature, banned or severely restricted?
- Are participants in peaceful demonstrations intimidated, arrested, or assaulted?
- Are online petitions, social media campaigns, and other forms of digital advocacy banned or severely restricted?

Freedom of association

- Are members of nongovernmental organizations (including civic organizations, interest groups, foundations, think tanks, gender rights groups, etc.) intimidated, arrested, imprisoned, or assaulted because of their work, particularly on human rights and governance?
- Are registration and other legal requirements for nongovernmental organizations particularly onerous or intended to prevent them from functioning freely?
- Are professional organizations, including business associations and trade unions, allowed to operate freely and without government interference?

Due process

- Is the judiciary subject to interference from the executive branch of government or from other political, economic, or religious influences?
Do executive legislative, and other governmental authorities comply with judicial decisions, and are those decisions effectively enforced?

Are defendants’ rights, including the presumption of innocence until proven guilty, protected?

Do law enforcement and other security officials operate professionally, independently, and accountably?

**Personal security**

- Do law enforcement officials beat detainees during arrest or use excessive force or torture to extract confessions?
- Do citizens have the means to effective petition and redress when they suffer physical abuse by state authorities?
- Is violence against various marginalized communities considered a crime, is it widespread, and are perpetrators brought to justice?
ENDNOTES

2 General Data Protection Regulation (GDPR), Article 4, https://gdpr-info.eu/art-4-gdpr
3 General Data Protection Regulation (GDPR), Recital 26, https://gdpr-info.eu/recitals/no-26-
4 General Data Protection Regulation (GDPR), Article 9, https://gdpr-info.eu/art-9-gdpr
5 General Data Protection Regulation (GDPR), Recital 53, https://gdpr-info.eu/recitals/no-53-
6 Data Protection in Turkey,” KVKK, https://kvkk.gov.tr/SharedFolderServer/CMSServer/CMSServerFiles/c02cb3c-7cc0-4f00-b0a7-8cc89089df8.pdf
7 Bill No. 373 of 2019, Art 3(28), (36), http://164.100.47.4/BillsTexts/LSBillsTexts/AsIntroduced/272_2019_LS_Eng.pdf;
9 Republic Act No. 10173, Art 3((g),(l), http://www.officialgazette.gov.ph/2012/08/12/republic-act-no-10173/
12 California Consumer Privacy Act of 2018, §1798.140(o), http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter&article
23 Judgement of the Court, Sec. 184 http://curia.europa.eu/jure/document/document.jsf;sessionid=c816a66cCfDoD08EB0C41C5400AsY7C7ctxes&docid=28677&pagexindex=0&doclang=EN&mode=reqdir&ir=0&cc=first&part=1&c=81912
26 Several initiatives have informed our thinking when developing these criteria. We recommend consulting these initiatives to create a more detailed assessment tool to evaluate the human rights risks resulting from data localization requirements:
34 Countries are ranked according to their Internet freedom scores assigned by Freedom House: https://freedomhouse.org/countries/freedom-net/scores
USER PRIVACY OR CYBER SOVEREIGNTY?
Assessing the human rights implications of data localization


See, for example, Andrei Soldatov and Irina Borogan, The Red Web, Public Affairs, 2015.


