Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security

TATEVIK SARGSYAN
American University, USA

Due to the increased awareness of the politics embedded in Internet technologies, there has been a growing tendency for state and nonstate actors around the world to leverage Internet infrastructure configurations to attain various political and economic objectives. Governments push for infrastructure modifications in pursuit of economic development, data privacy and security, and law enforcement and surveillance effectiveness. Information intermediaries set and enact their infrastructure to maximize revenue by enabling data collection and analytics, but have the capacity to implement tools for protecting privacy and limiting government surveillance. Relying on a conceptual framework of the politics of infrastructure, this article explores tensions and competing interests that emerge around intermediaries' technical and policy infrastructure through analysis of (a) data localization strategies in a number of countries and (b) privacy and security undertakings by information intermediaries.

Keywords: privacy, security, Internet infrastructure, surveillance, data localization

The Politics of Infrastructure

Governments across the world have come to recognize the importance of information intermediaries' infrastructure for national security, public safety, and other political interests. Law enforcement and intelligence agencies are tasked with addressing various challenges, including the growth of terrorism, cyberattacks, cybercrime, fraud, and—in some regimes—political opposition and social movements. To pursue these goals, government agencies often need to access communications data that are beyond their immediate control, facilitated by a handful of information intermediaries. These companies mediate content by providing online services and communication platforms to global users. In the meantime, their policy and technical infrastructure transcend geographic borders, challenging bureaucratic state power. Governments no longer have the ability to easily enforce laws, manipulate data and information flow, and secure privacy and security without relying on intermediary companies' infrastructure. Nation-states increasingly access user data by imposing law enforcement requests on information intermediaries such as search engines, social media, and e-mail platforms. They also conduct surveillance and establish control by cooperating with or pressuring companies in charge of communication infrastructure to allow access to data (Deibert, 2013; DeNardis, 2014; Fuchs, 2010).

Tatevik Sargsyan: ts0649a@student.american.edu
Date submitted: 2015–02–28

With few exceptions, major information intermediaries to whom global users entrust their private communication data are headquartered in the United States (e.g., Facbook, 2015; Google, 2015). Consequently, these companies assist in the collection and disclosure of data to law enforcement and intelligence agencies in the United States in accordance with various information policies. Moreover, under pressure, these Internet companies may agree to compromise encryption standards and allow backdoor access to data, subjecting global users' privacy to unwarranted surveillance. In 2013, for example, National Security Agency (NSA) consultant Edward Snowden revealed a number of surveillance programs that the NSA conducted in cooperation with information intermediaries, including Microsoft, Google, and Apple (Ball, 2013; Greenwald, 2013). These programs allegedly granted the U.S. government agencies with a direct access to communications data of intermediaries' global users, politicians, and various corporations. Ultimately, the U.S. government tried to advance its interests with the help of intermediary companies' communication infrastructure (Greenwald, MacAskill, Poitras, Ackerman, & Rushe, 2013; MacAskill, 2013).

Snowden's revelations and their widespread media coverage brought more awareness to the economic and political interests that are rooted in private intermediaries' infrastructure and encouraged many governments to similarly employ infrastructure to their political ends by proposing data localization initiatives. Data localization commonly encapsulates requirements that data be physically stored within a country's jurisdiction and/or not to be transferred abroad (e.g., Chander & Le, 2015; Hill, 2014). Effectively, data localization proposals urge companies to alter their infrastructure by relocating or building new data centers in specific locations.

Whereas users may access online services provided by major intermediaries such as Google, Amazon, Yahoo!, and Microsoft almost anywhere in the word, their data are transferred and stored in few geographically disproportionate data centers, allowing select governments to claim jurisdiction over the data and access them by imposing various surveillance laws (Lee, 2014). Such arrangements enable private companies to choose the optimal legal and economic environment for their operation while simultaneously making it difficult for many governments to access data located beyond their jurisdiction or safeguard privacy and security of users (Wood, 2014). Thus, some states have proposed data localization to eliminate privacy and security risks that exist due to foreign intelligence surveillance. Others have leveraged the public outrage and the heightened privacy concerns caused by the NSA spying to extend their control over data and their surveillance potential by data localization.

Relying on a conceptual framework that ascribes power and politics to infrastructure configurations (DeNardis, 2012; Lessig, 1999), in this article, I examine cases of data localization in contrasting legal environments such as China and Russia and France and Germany and policies and technical standards employed by information intermediaries. My goal is to demonstrate the political nature of infrastructure by examining the outcomes of its various uses and arrangements for surveillance and privacy and security of users.

Not only can infrastructure be designed to embrace specific values, but also its deployment can lead to many intended and unintended social consequences (Winner, 1980). From the early days of the Internet, privacy protection greatly depended on the careful technological design choices that engineers made and on prioritizing certain policy principles over others (Braman, 2012; DeNardis, 2009). In the modern information ecosystem, similarly, intermediaries' policies and technical choices have significant impact on privacy and can determine what intervention may be applied to their infrastructure. Whether data are accessible by governments is often determined by the encryption and privacy design choices companies make, by their data collection and retention policies, and their decisions to agree to government surveillance terms and to comply with law enforcement requests (DeNardis & Hackl, 2015; Soghoian, 2010).

What this means is that information intermediaries' infrastructure consisting of privately imposed policies and technical tools can be modified to embrace optimal privacy and security conditions for users. By embedding strong privacy and security features into their communication systems, intermediaries can simultaneously limit governments' means of accessing data illegally or through broad surveillance laws. For example, Internet companies can proactively design privacy-centric values into their infrastructure. This approach is called *privacy by design* and relies on the principle of building privacy into all phases of software development, from conception to implementation (Cavoukian & Jonas, 2012; Rubinstein & Good, 2013).

Privacy of users can also be strengthened by developing applications and tools that can be incorporated into already functional communication infrastructure such as encryption and anonymization systems to limit governments' access to data (Goldberg, 2003; Soghoian, 2010). Implementing technical solutions to privacy and security issues can increase the cost of conducting business and provision of free services to customers. Nevertheless, under mounting pressure, many information intermediaries have taken steps to address rising privacy issues for their long-term success and continued revenue, which depend on users' trust in the company practices.

The power and political nature of Internet infrastructure, however, is embedded not only in the ability to design and add privacy values into the underlying technologies and policies, but also in the ability to repurpose infrastructure for roles that it was not initially designed for. Internet infrastructure today hosts a growing economy of online commerce, international trade, and a global system of communication. However, the tools and technologies composing the Internet that have made decentralized information exchange possible and have greatly contributed to democratic values and economic growth have also become essential instruments to establish control and enable law enforcement and surveillance.

Data localization is one of the series of attempts by state actors to configure intermediaries' private infrastructure for their political goals, such as provision of privacy and security or easy access to data for legitimate and illegitimate reasons. However, the analysis of data localization cases in this article suggests that storing data on local servers may increase the effectiveness of law enforcement, grant governments more jurisdictional control over data, and amplify governments' surveillance potential, but it will do very little to safeguard privacy and security of users despite such claims by governments. Hence, stakeholders who are genuine about pursuing privacy and security protection for users may want to direct their efforts toward setting meaningful universal standards for policies and technical infrastructure of private companies to limit unauthorized surveillance instead of promoting disintegrated rules via data localization.

States, Data Localization, and Infrastructure Configurations to Enhance Surveillance, Privacy, and Security

Information intermediaries make information exchange possible among users via online services such as search engines and social media applications (DeNardis, 2014; Goldsmith & Wu, 2006). Due to their primary role in facilitating communication among Internet users and having access to user data, Internet intermediaries and their infrastructure are considered a natural point of control by governments (Balkin, 2014; DeNardis, 2012). Governments around the world continuously attempt to pass information policies to obtain user data aggregated by private companies for operational and commercial purposes. In July 2014, for example, the UK government introduced the Data Retention and Investigatory Powers Act requiring that companies retain the communications data of their users for up to 12 months. The data are to be made available to law enforcement for criminal or terrorist-based investigations. In 2015, the High Court ruled that the Data Retention and Investigatory Powers Act is illegal and has given the UK government until March 2016 to modify it (Bowcott, 2015; Travis, Wintour, & MacAskill, 2015). France also has made legal provisions that set the rules for intelligence agencies’ access to e-mails, Internet activity, personal location data, and other electronic communications (Chrisafis, 2015). In the United States, intelligence agencies may collect information on terrorists and enemies without a warrant if their communication takes place abroad. Surveillance authority over communication occurring or transiting via the United States is granted by the Foreign Intelligence Surveillance Amendments Act (Rosenbach & Peritz, 2009).

Large information intermediaries provide communication platforms to millions of users globally and generally observe the laws of the countries where they have physical operations (Goldsmith & Wu, 2006). This means that countries that host intermediaries’ data centers and offices have more opportunities to exercise influence over companies’ decisions and claim jurisdiction over data stored in their territory. Through a variety of laws and policies, governments delegate the burdensome task of surveillance to private intermediaries and expect their assistance in investigations, law enforcement, and espionage (Balkin, 2014). Companies with many users and services such as Microsoft, Google, and Facebook have teams whose job is to review data requests filed by law enforcement and make decisions about data disclosure (Deibert, 2013; Soghoian, 2012). Between January and June 2014, Google alone received 35,000 data requests by governments around the world (Google, 2014).

In addition, these companies are informally urged by government agencies to compromise their security infrastructure and/or not to implement strong security protocols to facilitate state surveillance. Similar arrangements between American Internet companies and the U.S. government became evident by the Snowden revelations (Greenwald, 2014), encouraging many foreign states to turn to local data storage requirements.

Following the revelations about the NSA surveillance programs, there has been growing consensus among governments that data localization and reliance on domestic infrastructure will safeguard privacy and security of citizens, especially against obtrusive foreign intelligence. A number of foreign countries have considered data localization initiatives that range from bypassing the U.S. and UK routing systems and undertaking development of local infrastructure to requiring that foreign information intermediaries create local data storage infrastructure (Chander & Le, 2015; Hill, 2014). Russia, China, South Korea, France, and Germany are among the countries promoting data localization.

Governments pursue data localization measures for a variety of reasons, stated and unstated. Some are really dedicated to providing better privacy protection to their citizens. Others rely on citizens' heightened privacy concerns to pursue alternative objectives, such as increasing their own law enforcement and intelligence effectiveness. Regardless of the purpose, data localization is yet another attempt by governments to repurpose infrastructure that makes global communication possible for alternative goals.

Data Localization in China

Even before the NSA mass surveillance revelations occurred, countries such as Russia, China, and Iran had spoken against the world's overreliance on the U.S. communication infrastructure and promoted the idea of jurisdiction-determined subnets (Mueller, 2010, 2011). In September 2011, the permanent representatives of China, Russia, Tajikistan, and Uzbekistan submitted a proposal to the United Nations General Assembly regarding information security code. The code itself did not reach consensus, but it characterized the ambitions of those states to ascribe authority for Internet-related public issues to the states as opposed to other stakeholders. Moreover, the code asserted that sovereign nations should have jurisdiction over digital data generated by their citizens and a right to thwart the dissemination of information that incites terrorism, secessionism, or extremism, as well as the right to protect their critical information infrastructure from threats (Polatin-Reuben & Wright, 2014; Smith, 2011).

For many years American intermediaries have intentionally avoided locating servers in repressive regimes so as not to be subject to laws that violate international human rights norms. In 2010, when Google decided to leave China, it attributed its decision to the cyberattacks, surveillance, and censorship by the Chinese authorities (Lohr, 2010). The move was followed by then U.S. Secretary of State Hilary Clinton's famous speech on Internet freedom. In Clinton's speech, China came up multiple times as a country that spikes threats to the free flow of information and co-opts Internet infrastructure to silence people. Clinton (2010) highlighted the need to have a single Internet and to allow all of humanity equal access to knowledge and ideas.

Three years later, an NSA surveillance scandal revealed the hypocrisy of the U.S. government. Coveted under a terrorism prevention narrative, the U.S. government had abused its privileged position in the Internet infrastructure and cooperated with U.S.-based companies for self-interests (Greenwald, 2014). China, a target of extensive NSA surveillance, including the creation of back doors in Huawei networks, asserted that American authorities had conducted large-scale cyberespionage against government officials, companies, and individuals. As a result, Chinese national discourse revolved around protecting data from surveillance of foreign countries. The Chinese government particularly expressed concern about security of the data stored in the cloud, outside of China, where it has no physical access and legal control over it (Polatin-Reuben & Wright, 2014).

The revelations served as a perfect opportunity for China to further the progress of data localization to ensure security, have stronger legal claim over data, and be able to manipulate and control communication. In 2013, the Chinese government published the *Information Security Technology Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems*. The guidelines establish basic principles for processing personal information and provide fundamental safeguards for data protection ranging from acquiring consent from users to using the information within the stated purposes. However, these 2013 guidelines, which apply to Internet intermediaries, also set out strong restrictions on data export and transfer without express consent and explicit regulatory approval. Although the guidelines are voluntary, they could serve as a regulatory framework for Chinese authorities and lawmakers (Greenleaf & Tian, 2013).

Cybersecurity concerns due to foreign intelligence continue to gain attention in China. In 2015, the Chinese government asked U.S. Internet intermediaries, in a letter, to commit to storing Chinese user data within the country’s borders and not to harm China’s national security. However, privacy and security groups have suggested that the language in the letter implies that Chinese authorities should have access to communication systems of American companies (Mozur, 2015a). Apart from the letter, China proposed an antiterrorist law, which requires communication companies to store Chinese user data on local servers and assist officials with access to communication (Mozur, 2015b). Thus, data localization initiatives in China are a response to the distrust toward U.S. intelligence and heightened cybersecurity concerns. At the same time, they further enhance the government’s surveillance power by configurations of intermediaries’ infrastructure.

Data Localization in Russia

Russian officials have also echoed the idea that design and administration of technical aspects of the Internet are directly linked to governments’ economic and political power and abilities to maintain control over communication. Russia has accused the United States and its allies of exploiting their dominant position in Internet infrastructure for geopolitical and economic objectives, including cybertheft (Banks, 2014). Through the years, Russia actively opposed the status quo administration of Internet infrastructure and multistakeholder approaches to Internet governance. It spoke against the Internet Corporation for Assigned Names and Numbers administering the domain name systems, arguing that the U.S. government assigns control of critical Internet resources to an organization that best represents its policy preferences (Mueller, 2010).

In 2012, Russia was among the countries proposing that United Nations member states be given equal rights to manage critical Internet resources (“Russia Backtracks,” 2012). The proposal, however, was abandoned after being met with strong opposition from the United States and other Western countries during and following the International Telecommunication Union conference and World Conference on International Telecommunications (Musil, 2012). With the strong campaign by the U.S.

technology industry, the civil society, and the U.S. government, the proposal was framed in the media as a threat to Internet freedom (Gross, 2012; Musil, 2012; Pfanner, 2012).

As the NSA surveillance details unfolded, Russian authorities leveraged the outcry to create new regulation for data collection and storage by Internet companies. Concerned with American companies passing data to U.S. law enforcement and intelligence agencies, the Russian government enacted a data localization law—Law 242. It went into effect on September 1, 2015, and mandates Internet intermediaries to save and process Russian user data on servers placed in the territory of the Russian Federation. The law also requires foreign companies to install state-provided encryption tools into their communication systems (Tymczyszyn & Zetoony, 2015).

Russia's aggressively growing practice of censorship and surveillance leads to the speculation that the government seeks self-interest by enacting the new law, in addition to addressing security and privacy concerns. Since Vladimir Putin's reelection in 2012, the Russian government has increased restrictions targeting the Internet. Federal Law 139, for example, deems publication of extremist material illegal in Russia and serves as a tool of censorship (Freedom House, 2014; Soldatov & Borogan, 2013). The Russian regulatory authority easily places oppositional websites deemed as harmful and extremist on an internal blacklist, which Internet service providers are required to block without prior decision or court approval. Citing the same law, authorities also turn to American intermediaries with censorship requests. Blocking access to information has become the Russian government's most common method to restrict user activity on the Internet (Gutterman, 2014). The Russian government has framed data localization as a necessary security measure. However, it also extends the government's surveillance potential and accelerates access to data managed by foreign companies, whose servers have traditionally been located outside Russian territory.

Data Localization in France and Germany

Privacy and security concerns sparked by the NSA data collection programs have led France and Germany to consider data localization by creating European communication networks and by urging American companies to store Europeans' data locally. Officials in these countries have proposed to reroute data traffic to bypass the U.S. and UK communication systems and to create a "Schengen area routing" to permit free exchange of data among Schengen states (Seiffert, 2014). French officials have expressed preference for locating data servers inside the country as a security and privacy measure, and even proposed to tax exploitation of data with the knowledge that many U.S.-based companies' activities can qualify as such. The cloud-computing company Cloudwatt has also been promoting local data storage in France (Ryan, Falvey, & Merchant, 2013; "Atos CEO," 2013).

The October 2015 decision by the Court of Justice of the European Union to revoke the Safe Harbor agreement, a legal regime regulating data transfer between the European Union and the United States, caused additional concerns about privacy safeguards of European citizens. Due to the perception that without Safe Harbor American companies cannot provide adequate privacy protection to European users, German data protection officials stated that those companies should consider storing data only on EU-based servers in the future (Drozdiak, 2015). France's and Germany's effort to provide privacy to their citizens and secure user data from unwarranted access by foreign intelligence is a legitimate objective. However, storing data locally does not necessarily mean better security and privacy conditions for users.

Days after Snowden's revelations, *Le Monde* newspaper disclosed that France has a large data collection program with minimal oversight. The General Directorate for External Security surveils all data transmissions in and out of France, including telephone calls, e-mails, and social media activity (Erlanger, 2013). Furthermore, in 2013, French legislators passed a new law that expands electronic surveillance of the country's residents and corporations for "national security," the protection of France's "scientific and economic potential," and prevention of "terrorism" or "criminality" with no judicial oversight (Sayare, 2013).

The German intelligence agency Bundesnachrichtendienst (BND) and NSA have extensively collaborated on their surveillance efforts. Germany agreed to collaborate with U.S. intelligence after the terror attacks on U.S. soil in 2001, and accordingly shares data on telephone calls, messages, e-mails, and so on, with the NSA. Between 2012 and 2013 alone, German intelligence supposedly sent about 72 million data items to the United States ("Spying Together," 2014). *Der Spiegel* ("Governments and NGOs," 2015) also reported that BND collected intelligence on state institutions, nongovernmental organizations, and various enterprises representing the interests of its allies. BND spied on foreign embassies and consulates located in Germany, the interior ministries of EU member states, Oxfam, the Red Cross, and the French–German enterprise Airbus Group, among others. Moreover, BND played a leadership role in WHARPDRIVE, a joint operation among NSA, BND, and a third partner that intercepted fiber optic cables to access international communications data.

Considering the existence and growth of broad surveillance programs in France and Germany and the data-sharing among intelligence agencies, it is unlikely that data localization proposals will lead to desired privacy and security outcomes. However, constructing local Internet infrastructure will make it easier for intelligence agencies and law enforcement to access data and will allow local Internet communication companies to establish a stronger position in the market dominated by American companies. Hence, for Germany and France, data localization opens economic and political opportunities.

Consequences of Data Localization

Safeguarding privacy and security is an essential pursuit for governments. However, the growing consensus among governments that data localization and domestic infrastructure will provide better privacy and security to citizens requires scrutiny. Many countries that have proposed to store data domestically also execute extensive surveillance, often with little oversight. The surveillance potential of these countries would greatly grow from access to localized data about citizens' social, economic, and political activities. Moreover, even in states such as Germany and France, where privacy laws are stricter, they can be overridden to prioritize national security and public safety interests (e.g., Sayare, 2013; Soldatov & Borogan, 2013).

Arguments that data localization will thwart foreign intelligence activities are also subject to question. Surveillance efforts are often directed at intercepting communication channels and hacking into data centers abroad. Hence, storing data on domestic servers will not prevent foreign agencies from conducting surveillance and espionage. In fact, centralizing data in one location makes it more vulnerable to hacking attacks and technical outages. More importantly, many governments such as Germany and the United States collaborate and share intelligence to address public safety and security issues, and storing data domestically will not inhibit the practice (e.g., "Spying Together," 2014).

Overall, centralized management of data will also increase human rights risks, especially in countries that lack strong legal systems. Without data storage and data transfer restrictions, information intermediaries are able to provide important platforms for free expression. However, having local operations will make these companies more vulnerable to censorship and surveillance demands, and will make information accessible to authorities for illegitimate reasons, risking the safety and privacy of minority groups, journalists, and activists.

Thus, it is far from clear that data localization can provide better privacy and security of data than what the current configuration of the Internet already offers. Data protection against unwarranted surveillance is not only conditioned by data location. It is also contingent on national security laws that grant excessive powers to law enforcement and intelligence agencies, as well as privacy and security safeguards built into communication infrastructure that can set limitations to surveillance possibilities across the world.

Information Intermediaries and Infrastructure Configurations to Limit Surveillance

Private information intermediaries' infrastructure of policies and tools also affects user privacy in a number of essential ways. First, these companies set the details of information collection, retention, and disclosure through their privacy policies (DeNardis, 2014). Second, through their decisions and technical choices, intermediaries mediate the possibilities for governments' access to user information. Despite government pressure to impose surveillance and national laws through intermediaries' infrastructure, these companies have flexibility in choosing optimal policies and tools for privacy and security protection.

For example, when users search on Bing or Google, Microsoft and Google collect, store, and analyze a broad range of information about users, including their Internet protocol address, cookie information, and search queries to improve services, prevent fraud, and profit from targeted advertising. Despite their usefulness, all these data can determine the location of computers and even reveal the identity of users. However, Google and Microsoft started deleting many identifiers associated with Web searches from their databases after six to nine months to provide some level of anonymity to users and simultaneously diminished the risks associated with unauthorized surveillance and data breaches (Google, 2008; O'Brien, 2010). This and similar data retention and deidentification policies can have positive implications for privacy protection of users, but rarely are embraced by companies because of their opportunity costs.

Companies also can fight unreasonable and unwarranted data requests and hold governments accountable by increasing transparency about law enforcement and intelligence agencies' requests. In 2014, a number of companies challenged the U.S. government in court and eventually received permission to share information about requests filed under the Foreign Intelligence Surveillance Amendments Act (Microsoft, 2014; Mimoso, 2014). The same year, a few information intermediaries involved in the PRISM program started notifying users whenever their data were the subject of a government request. According to some companies, the change of policy to notify users about subpoenas sometimes results in extraction of data requests filed by law enforcement (Albergotti, 2014). Microsoft also challenged U.S. law enforcement by refusing to disclose user data stored in Ireland based on a domestic search warrant (Lohr, 2014). Hence, being transparent and pushing back against government surveillance also can lead to fewer unwarranted privacy invasions. However, private intermediaries are not always eager to strain their partnerships with government agencies because of the understanding that governments may interfere in their economy with a threat of regulation and complication of business processes (Soghoian, 2011).

Apart from modifying data collection, retention, and disclosure policies, raising transparency, and challenging governments' surveillance practices, intermediaries can also rely on technology to provide privacy and security to users. Despite the fact that privacy and security measures may be in conflict with the business interests of these private companies, whose income depends on data collection and analysis, they can secure their communication systems by privacy-enhancing technologies and privacy by design. These applications and tools can be carefully designed and applied to increase privacy protection by enabling anonymity and confidentiality and by reducing possibilities for accessing and processing data (Cavoukian & Jonas, 2012; Pelkola, 2012; Rubinstein, 2011).

Companies can apply complex cryptographic features within their hardware and software systems to make stored data more secure and minimize unauthorized access (e.g., Apple, 2014). Information intermediaries can also implement various encryption protocols to secure communication as it travels between end users. For example, hypertext transfer protocol secure (i.e., https) can be applied to make information undecipherable during its transmission and, thus, invaluable to governments that intercept communication networks (Soghoian, 2010). In fact, the Snowden revelations have encouraged many companies including Facebook, Google, and Microsoft to employ various encryption protocols across their services (e.g., Meisner, 2013). Thus, considering the significance of information intermediaries' policies and tools for privacy and security, and their flexibility in setting and enacting policies and tools, it is necessary to seek not only favorable legal solutions to existing privacy and security concerns, but also solid industry standards.

Conclusion

Examination of information intermediaries' infrastructure for surveillance and privacy and security provision exemplifies its political nature and the growing tendency to resolve various political and economic objectives by infrastructure configurations. Companies and governments have vested interests in taking Internet infrastructure into a direction that benefits them. Governments ask intermediaries to modify infrastructure to pursue economic development, privacy and security, law enforcement effectiveness, enhanced surveillance, and the ability to track and oppress dissidents. Companies enact their policy and technical tools to maximize revenue by enabling data collection and analytics, and do not always prioritize users' privacy and security.

When evaluating attempts of states and private actors to make changes to infrastructure, stakeholders need to consider the values that the current Internet infrastructure brings to societies. The Internet's infrastructure and little legal intervention on data transfers across jurisdictions have helped create universal and interoperable networks of communication. These networks, in turn, promote access to knowledge and empower individuals to advocate for their rights. They also increase economic activity across jurisdictions by providing services to various industries, enabling digital trade, raising competition, and reducing costs.

There is no question that initiatives to repurpose and change infrastructure by data localization often stem from genuine concern for protecting privacy and security of users and fighting terrorism and adversaries. It is only fair that governments around the world want to have equal opportunity to apply national laws to the data of their citizens. For the majority of the commercial Internet history, only select governments have been able to impose local laws and claim jurisdiction over data stored in Internet companies' data centers. The United States has been particularly successful at using intermediary companies' resources for self-interests. Nevertheless, although data localization may facilitate law enforcement for some governments, overall, it will create obstacles to the free information flow and even contribute to surveillance and control in some states.

Private companies' information collection activities, cooperation with governments, and involvement in mass surveillance programs similarly harm users' privacy. Hence, there is a need to reevaluate the options for balancing companies' business needs, users' and governments' expectations for increased privacy safeguards, and governments' legitimate need to access data for law enforcement. In the meantime, stakeholders should pay attention to the policies and practices of intermediary companies as much as to regulations put forward by nation-states, and encourage implementation of privacy standards into intermediaries' technical and policy infrastructure. Deploying privacy-enhancing technologies and privacy by design to manage various elements of privacy and altering data collection, retention, and disclosure policies can uniformly and positively affect user privacy globally.

In addition, because privacy and security are not only a function of technological solutions, but also governments' ability to access data through overarching laws, technical "backdoors," and malware, stakeholders should continue to resist broad surveillance domestically and to increase transparency. Furthermore, it may be useful to create international norms capable of limiting states' powers to collect intelligence. States that are interested in alleviating the complexity of law enforcement by data localization may alternatively focus on Mutual Legal Assistance regime reforms and other international standards that can facilitate international cooperation on law enforcement requests.

References

Albergotti, R. (2014, May 2). Google, Microsoft, Apple to notify users about subpoenas in privacy nod. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424052702304677904579538320088504240

Apple. (2014). Government information requests. Retrieved from http://www.apple.com/privacy/government-information-requests/

Atos CEO says Schengen for data is no Maginot Line. (2013, November 26). Retrieved from http://www.telecompaper.com/news/atos-ceo-says-schengen-for-data-is-no-maginot-line--981970

Balkin, J. (2014). Old-school/new-school speech regulation. *Harvard Law Review, 127*(8), 2296–2342.

Ball, J. (2013, January 8). NSA's Prism surveillance program: How it works and what it can do. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

Banks, W. (2014, October). *Cyber espionage, surveillance, and international law: Finding common ground*. Paper presented at the Texas A&M Law Review Symposium, Fort Worth, TX.

Bowcott, O. (2015, July 17). High court rules data retention and surveillance legislation unlawful. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/jul/17/data-retention-and-surveillance-legislation-ruled-unlawful

Braman, S. (2012). Privacy by design: Networked computing, 1969–1979. *New Media & Society, 14*(5), 798–814.

Cavoukian, A., & Jonas, J. (2012). *Privacy by design in the age of big data*. Toronto, ON: Report of the Information and Privacy Commissioner. Retrieved from https://www.ipc.on.ca/images/Resources/pbd-big_data.pdf

Chander, A., & Le, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 667–739.

Chrisafis, A. (2015, May 5). France passes new surveillance law in wake of Charlie Hebdo attack. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack

Clinton, H. (2010, January 21). Remarks on Internet freedom. Retrieved from http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Deibert, R. (2013). *Black code: Inside the battle for cyberspace*. Toronto, ON: McClelland & Stewart.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society, 15*(5), 720–738.

DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

DeNardis, L., & Hackl, A. (2015). Internet governance by social media platforms. *Telecommunications Policy, 39*(9), 761–770. doi:10.1016/j.telpol.2015.04.003

Drozdiak, N. (2015, October 29). Germany's tough line on data transfers to U.S. is criticized. *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/brussels/2015/10/29/germanys-tough-line-on-data-transfers-to-u-s-is-criticized/

Erlanger, S. (2013, July 4). France, too, is sweeping up data, newspaper reveals. *The New York Times*. Retrieved from http://www.nytimes.com/2013/07/05/world/europe/france-too-is-collecting-data-newspaper-reveals.html

Facebook. (2015). Company information. Retrieved from https://newsroom.fb.com/company-info/

Freedom House. (2014). Freedom on the Net 2013. Retrieved from http://www.freedomhouse.org/report/freedom-net/2013/russia#.VFLfcGMiBp1

Fuchs, C. (2010). Web 2.0, prosumption, and surveillance. *Surveillance & Society, 8*(3), 288–309.

Goldberg, I. (2003). Privacy-enhancing technologies for the Internet: II. Five years later. In R. Dingledine & P. Syverson (Eds.), *Privacy enhancing technologies* (Vol. 2482, pp. 1–12). Berlin, Germany: Springer.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford, UK: Oxford University Press.

Google. (2008, September 8). Another step to protect user privacy [Web log post]. Retrieved from https://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html

Google. (2014). Google transparency report. Retrieved from http://www.google.com/transparencyreport/userdatarequests/countries/

Google. (2015). Company overview. Retrieved from https://www.google.com/intl/en_US/about/company/

Governments and NGOs: Germany spied on friends and Vatican. (2015, November 7). *Der Spiegel*. Retrieved from http://www.spiegel.de/international/germany/german-bnd-intelligence-spied-on-friends-and-vatican-a-1061588.html

Greenleaf, G., & Tian, G. (2013). China expands data protection through 2013 guidelines: A “third line” for personal information protection (with a translation of the guidelines). *Privacy Laws & Business International Report, 122*(1), 4–6.

Greenwald, G. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013, July 12). Microsoft handed the NSA access to encrypted messages. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Gross, G. (2012, May 31). U.S. tech leaders fear proposed Internet regulations, taxes at ITU meeting. *PCWorld*. Retrieved from http://www.pcworld.com/article/256596/ us_tech_leaders_fear_proposed_internet_regulations_taxes_at_itu_meeting.html

Gutterman, S. (2014, March 13). Russia blocks Internet sites of Putin critics. *Reuters*. Retrieved from http://www.reuters.com/article/2014/03/13/us-russia-internet-idUSBREA2C21L20140313

Hill, J. F. (2014). The growth of data localization post-Snowden: Analysis and recommendations for U.S. policymakers and industry leaders. *Lawfare Research Paper Series, 2*(3), 1–41.

Lee, T. B. (2014). Here’s where your data lives. *Vox*. Retrieved from http://www.vox.com/a/internet-maps#list-28

Lessig, L. (1999). *Code: And other laws of cyberspace*. New York, NY: Basic Books.

Lohr, S. (2010, March 22). Sergey Brin on Google’s China move. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2010/03/22/interview-sergey-brin-on-googles-china-gambit/?_r=0

Lohr, S. (2014, June 10). Microsoft protests order to disclose e-mail stored abroad. *The New York Times*. Retrieved from http://www.nytimes.com/2014/06/11/technology/microsoft-protests-order-for-email-stored-abroad.html

MacAskill, E. (2013, August 23). NSA paid millions to cover Prism compliance costs for tech companies. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

Meisner, J. (2013, December 4). Protecting customer data from government snooping [Web log post]. Retrieved from http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/#sm.00001qvg4dxux3cplsnp2z6nlqb4w

Microsoft. (2014, February 3). Providing additional transparency on U.S. government requests for customer data [Web log post]. Retrieved from http://blogs.microsoft.com/on-the-issues/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data/

Mimoso, M. (2014, January 28). Justice Department eases gag order on FISA, National Security Letter reporting. *Threatpost*. Retrieved from http://threatpost.com/justice-dept-eases-gag-order-on-fisa-national-security-letter-reporting/103903

Mozur, P. (2015a, September 16). China tries to extract pledge of compliance from U.S. tech firms. *The New York Times*. Retrieved from http://www.nytimes.com/2015/09/17/technology/china-tries-to-extract-pledge-of-compliance-from-us-tech-firms.html?_r=0

Mozur, P. (2015b, July 2). Jitters in tech world over new Chinese security law. *The New York Times*. Retrieved from http://www.nytimes.com/2015/07/03/business/international/jitters-in-tech-world-over-new-chinese-security-law.html

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Mueller, M. (2011). China and Internet governance. In J. Palfrey, R. Deibert, R. Rohozinski, & J. Zittrain (Eds.), *Access contested* (pp. 177–194). Cambridge, MA: MIT Press.

Musil, S. (2012, December 10). Russia abandons proposal for U.N. governance of Internet. *CNET News*. Retrieved from http://www.cnet.com/news/russia-abandons-proposal-for-u-n-governance-of-internet/

O’Brien, K. J. (2010, January 22). Microsoft puts a time limit on Bing data. *The New York Times*. Retrieved from http://www.nytimes.com/2010/01/20/technology/companies/20search.html?mtrref= www.google.com&gwh=0E29116B16767E3801ABF7B0C039915D&gwt=pay&_r=0

Pelkola, D. (2012). A framework for managing privacy-enhancing technology. *IEEE Software, 29*(3), 45–49.

Pfanner, E. (2012, June 11). Debunking rumors of an Internet takeover. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/11/technology/debunking-rumors-of-an-internet-takeover.html?pagewanted=all&_r=0

Polatin-Reuben, D., & Wright, J. (2014, August).. *An Internet with BRICS characteristics: Data sovereignty and the Balkanisation of the Internet.* Paper presented at the Fourth USENIX Workshop on Free and Open Communications on the Internet, San Diego, CA. Retrieved from https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben

Rosenbach, E., & Peritz, A. J. (2009). *Electronic surveillance and FISA*. Cambridge, MA: Belfer Center for Science and International Affairs. Retrieved from http://belfercenter.ksg.harvard.edu/publication/19156/electronic_surveillance_and_fisa.html

Rubinstein, I. S. (2011). Regulating privacy by design. *Berkeley Technology Law Journal, 26*(3), 1409–1456.

Rubinstein, I. S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Technology Law Journal, 28*(2), 1333–1413.

Russia backtracks on Internet governance proposals. (2012, December 11). Retrieved from http://www.bbc.com/news/20676293

Ryan, P. S., Falvey, S., & Merchant, R. (2013). When the cloud goes local: The global problem with data localization. *Computer, 46*(12), 54–59.

Sayare, S. (2013, December 14). France broadens its surveillance power. *The New York Times*. Retrieved from http://www.nytimes.com/2013/12/15/world/europe/france-broadens-its-surveillance-power.html?_r=0

Seiffert, J. (2014, Februaury 20). Weighing a Schengen zone for Europe's Internet data. *Deutsche Welle*. Retrieved from http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482

Smith, G. (2011, November 27). State Department official accuses Russia and China of seeking greater Internet control. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2011/09/27/russia-china-internet-control_n_984223.html

Soghoian, C. (2010). Caught in the cloud: Privacy, encryption, and government back doors in the Web 2.0 era. *Journal on Telecommunications and High Technology Law, 8*, 359–424.

Soghoian, C. (2011). An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government. *Minnesota Journal of Law, Science & Technology, 12*(1), 191–237.

Soghoian, C. (2012). *The spies we trust: Third party service providers and law enforcement surveillance* (Doctoral dissertation, Indiana University). Retrieved from http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf

Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal, 30*(3), 23–30.

Spying together: Germany's deep cooperation with the NSA. (2014, June 18). *Der Spiegel*. Retrieved from http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

Travis, A., Wintour, P., & MacAskill, E. (2015, November 4). Theresa May unveils UK surveillance measures in wake of Snowden claims. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden

Tymczyszyn, I., & Zetoony, D. A. (2015). Russia data localization requirement at a glance: Practical aspects. *Bryan Cave.* Retrieved from http://bryancavedatamatters.com/russia-data-localization-requirements-at-a-glance/

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121–136.

Wood, R. (2014, October 14). Ireland corks double Irish tax deal, closing time for Apple, Google, Twitter, Facebook. *Forbes*. Retrieved from http://www.forbes.com/sites/robertwood/2014/10/14/ireland-corks-double-irish-tax-deal-closing-time-for-apple-google-twitter-facebook/