LAWFARE RESEARCH PAPER SERIES

VOL. 2 **JULY 21, 2014** **NO. 3**

THE GROWTH OF DATA LOCALIZATION POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND INDUSTRY LEADERS *

Jonah Force Hill **

In the wake of the Edward Snowden intelligence disclosures, governments around the world are increasingly considering enacting so-called "data localization" policies, laws and guidelines which limit the storage, movement, and/or processing of digital data to specific geographies, jurisdictions, and companies. This paper analyzes the complex—and often overlooked—motivations behind the data localization movement, explains how localization policies (in all their various permutations) fail to achieve their stated goals, and highlights some of the many harms localization can cause. Recommendations are provided for U.S. business leaders and policymakers seeking to counter this problematic trend.

---

* A version of this paper was presented at the May 2014 "Global Governance of Cyberspace Conference" held at the Institute for Global Justice at The Hague.

** Jonah Force Hill is a San Francisco-based technology and international affairs consultant and a Fellow of the Global Governance Futures 2025 program. He has served in the Office of the Cybersecurity Coordinator at the White House, as a Cybersecurity Teaching Fellow at Harvard, and in the political affairs section of the U.S. Embassy in New Delhi. He holds an MPP from the Harvard Kennedy School of Government, where he was a fellow of the Belfer Center for Science and International Affairs, an MTS from Harvard Divinity School, and a BA from UCLA. The views expressed in this paper are his own.

Special thanks to Sameer Bhalotra, Scott Bradner, Laura DeNardis, Nils Gilman, Vivek Mohan, Paul Rosenzweig, and Ian Wallace for their thoughtful and invaluable assistance.

I. DATA LOCALIZATION

Over the course of recent decades, and principally since the commercialization of the Internet in the early 1990s, governments around the world have struggled to address the wide range of logistical, privacy, and security challenges presented by the rapid growth and diversification of digital data. The mounting online theft of intellectual property, the growth of sophisticated malware, and the challenges involved in regulating the flow, storage, and analysis of data have all—to varying degrees—increasingly challenged governments' ability to respond with effective policy.

Until recently, these data management issues were left to the men and women of computer science departments, advocates for technology companies, and to the few government attorneys and bureaucrats responsible for overseeing Internet and data regulation. In the wake of former NSA contractor Edward Snowden's disclosures, however, which revealed to the global public the scale and intensity of intelligence collection online, data security and privacy issues have now become front-page headlines and the topics of dinner-table conversation the world over. As a result, governments are increasingly feeling compelled to do something they see as meaningful—if not outright

drastic—to protect their citizens and their businesses from the many challenges they perceive to be threatening their nation's data and privacy.

Of the various responses under consideration, perhaps none has been more controversial—or more deeply troubling to American businesses—than the push to enact laws that force the "localization" of data and the infrastructure that supports it. These are laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal situs of operations and management. By keeping data stored within national jurisdictions, or by prohibiting data from traveling through the territory or infrastructure of "untrustworthy" nations or those nations' technology companies, the argument goes, data will be better protected, and surveillance of the kind orchestrated by the NSA curtailed.

Today, more than a dozen countries,[1] both developed and developing, have introduced or are actively contemplating introducing data localization laws. The laws, restrictions, and policies under consideration are diverse in their strategies and effects. Some proposals would enforce limitations for data storage, data transfer, and data processing; others require the local purchasing of ICT equipment for government and private sector procurements. There are proposals for mandatory local ownership of data storage equipment, limitations on foreign online retailers, and forced local hiring.

Proposals of this sort are not historically unprecedented. Indeed, forms of data localization policies have been actively in place in many countries for years, including in the United States, where sensitive government data, such as certain classified materials, must be maintained within the servers of domestic companies. Broader localization rules, which apply to *all* citizen data, have tended to be pursued by authoritarian governments such as Russia, China, and Iran, for which data localization laws have been viewed as an effective means to control information and to monitor the activities of their citizens.[2] Post-Snowden, however, even democratic countries are now seriously considering these more expansive data localization measures. Most notably, Brazil, Germany, and India—countries that have witnessed some of the most virulent anti-NSA reactions—are now contemplating enacting significant data

[1] For several good examples of the data localization trend around the world (in addition to other localization policies as barriers to trade), see Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, "Localization as Barriers to Trade: Threat to the Global Innovation Economy." *The Information Technology and Innovation Foundation*, September 2013, available at http://www.copyrightalliance.org/sites/default/files/resources/2013-localization-barriers-to-trade.pdf; see also "Business Without Borders: The Importance of Cross Border Data Transfers to Global Prosperity." *U.S. Chamber of Commerce and Hunton Williams*, 2014.

[2] For instance, the Great Firewall of China, the Chinese government's system of legal and technical Internet controls, is enabled through controls afforded by locally owned and operated servers. For coverage of the Great Firewall system, see https://en.greatfire.org/.

localization laws. The EU is also contemplating localization within its area of authority.[3]

This is a deeply troubling development—not just for the technology firms of the United States who stand to lose customers and contracts as a result of these policies,[4] but also for all the nations, firms, and individual Internet users who rely on the Web for economic trade and development, communications, and civic organizing. Not only do data localization policies fail to achieve their stated goals, they introduce a host of unintended consequences. By restricting data flows and competition between firms, localization will likely bring up costs for Internet users and businesses, may retard technological innovation and the Internet's "generativity,"[5] may reduce the ability of firms to aggregate services and data analytics through cloud services, and will surely curb freedom of expression and transparency globally. Ironically, data localization policies will likely degrade—rather than improve—data security for the countries considering them, making surveillance, protection from which is the ostensible reason for localization, easier for domestic governments (and perhaps even for foreign powers) to achieve. Restricted routing, often a core component of data localization rules, may be technically infeasible without initiating a significant overhaul of the Internet's core architecture and governance systems, which itself would have significant negative effects. And perhaps most worrying, data localization policies—if implemented on a wide international scale—could have the effect of profoundly fragmenting the Internet,[6] turning back the clock on the integration of global communication and ecommerce, and putting into jeopardy the myriad of societal benefits that Internet integration has engendered.

Unquestionably, online espionage, citizen privacy, government overreach, and the protection of fundamental rights are legitimate concerns of states and

---

[3] In addition, democratic countries such as Australia, Canada, France, and Malaysia are also considering variations of data localization rules. See Chander, Anupam and Le, Uyen P., "Breaking the Web: Data Localization vs. the Global Internet" (April 2014). *Emory Law Journal*, Forthcoming; UC Davis Legal Studies Research Paper No. 378, available at SSRN: http://ssrn.com/abstract=2407858.

[4] Boeing Reports that it lost out on a $4.5 billion contract with the Brazilian Air Force, a loss that was widely credited to the fallout of the NSA leaks. See Reuben F. Johnson, "Boeing Loses $4.5B Contract With Brazil, NSA Leaks Cited," The Washington Free Beacon, 16 January 2014, available at http://freebeacon.com/national-security/boeing-loses-4-5b-contract-with-brazil-nsa-leaks-cited/.

[5] "Generativtiy" can be defined "as a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences." See Jonathan L. Zittrain, "The Generative Internet," 119 Harv. L. Rev 1974 (2006).

[6] For more information on the concept and manifestations of Internet fragmentation, see Jonah Force Hill, "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers." Paper, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2012, available at http://belfercenter.hks.harvard.edu/publication/22040/internet_fragmentation.html?breadcrumb=%2Fpublication%2F17613%2Fgovernance_and_information_technology.

deserving of appropriate policy responses. Advances in surveillance technologies and offensive cyber capabilities have plainly outpaced the legal, normative, and diplomatic mechanisms needed to protect digital data. For government officials hoping to take meaningful action in response, data localization looks to be a convenient and simple solution. But a close examination reveals that it is not a viable remedy to any of the privacy, security, or surveillance problems governments hope to address. This paper discusses these points and seeks to expose the often dubious and pretextual motivations behind the new push for data localization, to explain how such measures are profoundly imprudent and often self-defeating, and to offer United States businesses and the United States government a few key recommendations for how to counter this problematic trend.

II. U.S. COMPANIES DEEMED UNTRUSTWORTHY

For a great many around the globe, the Snowden disclosures revealed a disturbing relationship between the major U.S. technology firms and the American national security establishment. Specifically, the disclosures showed that Yahoo, Google, and other large American tech companies had provided the NSA with access to the data of the users of their services. Although there were many programs that tied the major American firms to the NSA,[7] three in particular drew special ire: the much-discussed PRISM program,[8] a collaborative effort between the NSA and the FBI which compelled Internet companies to hand over data held within servers located on U.S. soil in response a subpoena issued by a special intelligence court, and two programs known as MUSCULAR and TEMPORA,[9] both of which allowed the NSA (in partnership with Britain's signals intelligence agency, the GCHQ) to access information transmitted through the data communication links of American-owned firms located outside the U.S., where statutory limitations on data collection are far less stringent.[10]

---

[7] For an excellent list of reported leaks to date, see "Catalog of the Snowden Revelations," *Lawfareblog*, available at http://www.lawfareblog.com/catalog-of-the-snowden-revelations/

[8] "PRISM: Here's how the NSA wiretapped the Internet" *ZDNET*, 8 June 2013, available at http://www.zdnet.com/prism-heres-how-the-nsa-wiretapped-the-internet-7000016565/.

[9] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say." *The Washington Post,* 30 October 2013, available at http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

TEMPORA, importantly, was a collaboration between the NSA and the British signals intelligence agency, the Government Communications Headquarters (GCHQ). See Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fiber-optic cables for secret access to world's communications," *The Guardian*, 21 June 2013, available at http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[10] The NSA collects data based primarily on four different legal authorities: the Foreign Intelligence Surveillance Act (FISA) of 1978, Executive Order 12333 of 1981 and modified in 2004 and 2008, Section 215 of the Patriot Act of 2001, and Section 702 of the FISA

The fact that American companies provided the U.S. government with information and access to data (knowingly in some cases, apparently unwittingly in others) has led many foreign leaders to conclude that only domestic firms—or at least non-American firms—operating exclusively within local jurisdictions, can be trusted to host the data of their citizens. Prominent political voices around the globe have been anything but subtle in their articulation of this assessment. Following the publication of the PRISM program in the *Guardian* newspaper, German Interior Minister Hans-Peter Friedrich declared that, "whoever fears their communication is being intercepted in any way should use services that don't go through American servers."[11] France's Minister for the Digital Economy similarly insisted that it was now necessary to "locate datacenters and servers in [French] national territory in order to better ensure data security."[12] Brazilian President Dilma Rousseff agreed, insisting that, "there is a serious problem of storage databases abroad. That certain situation we will no longer accept."[13]

Unsurprisingly, these declarations from government officials at the ministerial level and higher, and the policy responses those declarations suggest, are profoundly troubling to American technology companies. U.S. firms have issued dire warnings in response,[14] predicting that they could lose tens of billions of dollars in revenue abroad as distrustful foreign governments and customers move—either by choice or by legal mandate—to non-U.S. alternatives. Firms fear that the anti-American backlash, distrust in American

---

Amendments Act (FAA) of 2008, described by Bruce Schneier, "Don't Listen to Google and Facebook: The Public Private Surveillance Partnership is Still Going Strong." *The Atlantic*, 25 March 2014, available at http://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/; see also "Are they allowed to do that? A breakdown of selected government surveillance programs." *The Brennan Center for Justice* at New York University School of Law, available at http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf; John W. Rollins and Edward C. Liu, "NSA Surveillance Leaks: Background and Issues for Congress," *Congressional Research Service*, 4 September 2013, available at http://www.fas.org/sgp/crs/intel/R43134.pdf; The President Review Group on Communications and Technologies, "Liberty and Security in a Changing World," 12 December 2013, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[11] "German minister: drop Google if you fear US spying," *Associated Press*, July 3, 2013, available at http://news.yahoo.com/german-minister-drop-google-fear-us-spying-105524847.html.

[12] Valéry Marchive "France hopes to turn PRISM worries into cloud opportunities." *ZDNET* 21 June 2013, available at http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/.

[13] Michael Hickins, "NSA Spying Stymies U.S Tech Firms" *The Wall Street Journal*, 3 February 2014, available at http://online.wsj.com/news/articles/SB10001424052702303743604579350611848246 01.

[14] Claire Cain Miller, "Google Pushes Back Against Data Localization" *The New York Times, Bits and Bits Blog*, 24 January 2014, available at http://bits.blogs.nytimes.com/2014/01/24/google-pushes-back-against-data-localization/.

firms, and potentially resulting data localization laws (depending on the specifics of the rules enacted) will mean that they will be forced out of certain markets, or forced to build expensive—and oftentimes unnecessarily redundant—data centers abroad. Analysts are suggesting the fallout could mirror what happened to Huawei and ZTE, the Chinese technology and telecommunications firms that were forced to abandon some U.S. contracts when American lawmakers accused the companies of planting in their products coding "backdoors" for the Chinese People's Liberation Army and intelligence services.[15] A much-cited estimate[16] by the Information Technology and Innovation Foundation, an independent think-tank, confirmed American tech firms' worst fears when it opined that the U.S. cloud computing industry alone could lose between $21.5 billion and $35 billion over the next three years as a result of the NSA backlash.[17]

In an attempt to stem the data localization trend, U.S. firms and trade associations have launched a multi-pronged campaign to regain the trust of foreign governments and customers. Intense lobbying efforts are underway to reform U.S. surveillance laws,[18] which have been viewed as overly permissive with regard to governmental collection of data, and to highlight the many ways that localization could harm economic competitiveness and growth.[19]

---

[15] Tom Risen, "Chinese Telcom Huawei Will Exit the U.S. Market" *USNews*, 3 December 2013, available at: http://www.usnews.com/news/articles/2013/12/03/chinese-telecom-huawei-will-exit-the-us-market.
Joann S. Lubin and Shandi Raice, "Security Fears Kill Chinese Bid in U.S." *The Wall Street Journal*, 5 November 2010, available at http://online.wsj.com/news/articles/SB10001424052702303789604579198370093354 68.

[16] The President's Review Group used the ITIF study in their discussion of localization, as well. President's Review Group, Ibid.

[17] This number is only a rough estimate since the exact terms of the localization proposals are still up for debate and few companies have stated publically that they have lost contracts since the Snowden episode, but the fact that it has been so widely cited suggests that it reflects a somewhat realistic assessment of the potential impact. Daniel Castro, "How Much Will PRISM Cost the US Cloud Computing Industry," *ITIF*, August 2013 (estimating monetary impact on US cloud providers of $21.5 billion by 2016, based on 10% loss in foreign market share), available at www2.itif.org/2013-cloud-computing-costs.pdf.

[18] Craig Timberg, "Major tech companies unite to call for new limits on surveillance." *The Washington Post*, 8 December 2013, available at http://www.washingtonpost.com/business/technology/major-tech-companies-unite-to-call-for-new-limits-on-surveillance/2013/12/08/530f0fd4-6051-11e3-bf45-61f69f54fc5f_story.html. "Cisco calls for curb on NSA surveillance efforts," *BBC*, 19 May 2014, available at http://www.bbc.com/news/technology-27468794.

[19] "Safeguard Cross Border Data Flows," *U.S. Chamber of Commerce Issue Brief*, available at https://www.uschamber.com/issue-brief/safeguard-cross-border-data-flows; "Letter on the Marco Civil," *ITIF*, 5 August 2013, available at http://www.itic.org/dotAsset/2a6d7008-9c61-4f7c-917a-5fe4ad493527.pdf; "Letter to the Brazilian Congress," *Wilson Center*, 22 October 2013, available at http://www.wilsoncenter.org/sites/default/files/Data%20Center%20Localization%20-%20English%20version.pdf.

Domestically, Microsoft[20] and Google, joined by Apple, Facebook and other firms, successfully sued the U.S. government in order to gain legal authority to provide the public greater detail on the information the U.S. government collects from them.[21] Google's Eric Schmidt, Facebook's Mark Zuckerberg, Netflix's Reed Hastings, and the leaders of Dropbox, Palantir, and other top tech executives met with President Barack Obama in March 2014, to discuss potential surveillance reforms.[22] IBM is reportedly spending more than a billion dollars to build 15 new data centers overseas in an effort to preempt formalized localization rules.[23] Salesforce.com, a major cloud services provider, has announced similar plans.[24] And in the U.S. courts, Microsoft has challenged the authority of federal prosecutors to compel release of email records stored in an overseas data center in Ireland, marking the first time a major U.S. tech company has challenged a domestic search warrant requesting digital information of its customers abroad.[25]

---

[20] Brad Smith (Microsoft General Counsel and EVP), "Standing together for greater transparency." Public letter to Microsoft users. 30 August 2013 http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx.

[21] Tony Romm, "Google, others more NSA transparency." *Politico*, 27 January 2014, available at http://www.politico.com/story/2014/01/barack-obama-administration-nsa-national-security-agency-tech-technology-transparency-eric-holder-james-clapper-102677.html; Original case: Craig Timberg and Cecilia Kang, "Google challenges U.S. gag order, citing First Amendment." *The Washington Post*, 18 June 2013, available at http://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html; Firms are increasingly revealing requests for data without prior government approval, see Craig Timberg, "Apple, Facebook, others defy authorities, notify users of secret data demands," *The Washington Post*, 1 May 2014, available at http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?hpid=z1.

[22] Tony Romm, "Mark Zuckerberg, other tech execs meet with Barack Obama." *Politico*, 21 March 2014, available at http://www.politico.com/story/2014/03/mark-zuckerberg-barack-obama-tech-ceos-nsa-104907.html?hp=l14.

[23] Tony Kontzer, "IBM Spends $1.2 Billion on New Cloud Datacenters." *NetworkComputing*, 23 January 2014, available at http://www.networkcomputing.com/next-generation-data-center/news/servers/ibm-spends-12-billion-on-new-cloud-dat/240165593. Claire Cain Miller, "Revelations of NSA spying cost U.S. tech companies." *The New York Times*, 21 March 2014, available at http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Nick Wingfield and Mark Scott, "Microsoft suggests wider options for foreign data." *The New York Times*, 23 January 2014, available at http://bits.blogs.nytimes.com/2014/01/23/microsoft-suggests-wider-options-for-foreign-data/?_php=true&_type=blogs&_r=0.

[24] Chris Kanaracus, "Salesfore.com to add three data centers in Europe." *PC World*, 3 March 2014, available at http://www.pcworld.com/article/2103900/salesforcecom-to-add-three-data-centers-in-europe.html.

[25] Microsoft argues that the United States should abide by its mutual legal assistance treaty obligations, here by seeking prior authorization from an Irish court before obtaining the data. The United States, on the other hand, argues that its request is in line with the Electronic Communications Privacy Act, and that the location of the data is irrelevant: the company is

III. LOCALIZATION PROPOSALS

It remains to be seen whether lobbying, litigation, or technical responses will salvage the overseas reputations of the American tech companies, or protect their market shares abroad. Data localization proposals continue to be floated and seriously considered in several major markets crucial to the companies' bottom lines.

The problem for U.S. tech companies is that there are actually a wide variety of forces and interest groups driving the data localization movement, and many of these forces and groups have objectives beyond the professed goals of data protection and counter-NSA surveillance. One can easily discern in foreign governments' interest in data localization a combination of anti-American populism, a desire for greater ease of foreign (and domestic) surveillance, and a sense among policymakers and business that the Snowden backlash presents an opportunity to cultivate domestic cloud and other tech services industries, industries that have long been outcompeted by American tech companies in their home markets—old-fashioned protectionism tailored for the digital age.

A quick look at four select localization studies[26] reveals this complex mix of purposes, and helps to explain why U.S. technology firms—as well as those organizations and individuals abroad who also recognize the problems data localization laws would introduce—are having such a difficult time arguing their case, despite the logic working in their favor and against the policies they are contesting.

A. *Germany and "Schengen Area" Routing*

Among the many countries riled by the Snowden revelations, perhaps none has been more vocal in its condemnation, or appeared to have been more profoundly aggrieved by the NSA surveillance programs, than Germany. The reasons for the Germans' unique outrage over the NSA programs are complex, but much of the explanation is historical. Germany is a society still deeply scared by its national memories of the surveillance tactics used by both the Nazis during WWII and the East German Stasi during the Cold War. The NSA

---

an American one, and thus properly subject to search without any additional, treaty-based process. Oral arguments on the matter are scheduled for July. Edward Moyer, "Microsoft fights US warrant for customer data stored overseas." *CNET*, 11 June 2014, available at http://www.cnet.com/news/microsoft-fights-us-warrant-for-customer-data-stored-overseas/ and Ellen Nakashima, "Microsoft fights U.S. search warrant for customer e-mails held in overseas server." *The Washington Post*, 10 June 2014, Available at http://m.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html?tid=HP_more

[26] The focus here is on democratic countries, but business is hurting in non-democratic nations such as in China as well. See Spencer E. Ante, Paul Mozur, and Shira Ovide, "NSA Fallout: Tech Firms Feel a Chill Inside China," The Wall Street Journal, 14 November 2013, available at http://online.wsj.com/news/articles/SB10001424052702303789604579198370093354 68.

surveillance dragnet has triggered painful memories of those eras and ignited a call for swift action in Berlin. Chancellor Merkel, whose anger overwhelmed her understanding of history, has even gone so far as to make a NSA-Stasi parallel in a conversation with President Obama following disclosure that the NSA had been tapping her phone conversations.[27]

In modern Germany, data privacy has become virtually sacrosanct. Even before the Snowden revelations, German data protection commissioners had developed a track record of filing suits against U.S. Internet companies such as Facebook, Google, and the Wikimedia Foundation, challenging data collection, transfer, and use practices that, while commonly accepted in other countries, are vigorously protested and questionably legal in Germany.[28] Germany's highest court has gone so far as to establish a constitutional right to "integrity and confidentiality of IT systems."[29]

It should have come as no surprise, then, that the Germans have serious misgivings about the probity of American tech companies following the Snowden disclosures, and that the German government would develop and pursue strategies to address the concerns of its citizens. And indeed it is devising such strategies. Among a host of actions, including a request for U.S.-German "no-spy" agreement[30]—which has since been rejected by the Obama administration[31]—German authorities are considering data localization in a

---

[27] Germany Chancellor Angela Merkel confronted Obama with the statement: "This is like the Stasi." Ian Traynor and Paul Lewis "Merkel Compared NSA to Stasi in Heated Encounter with Obama" The Guardian, 17 December 2013, available at http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama.

[28] Heather Horn, "Germany's War with Facebook and Google over Privacy," *The Atlantic*. 2 December 2011: http://www.theatlantic.com/international/archive/2011/12/germanys-war-with-facebook-and-google-overprivacy/248914/; "Facebook violates German law, Hamburg data protection official says," *Deutsche Welle*. 8 February 2011: http://www.dw.de/facebook-violates-german-law-hamburg-data-protection-official-says/a-15290120; Tristana Moore, "Facebook Under Attack in Germany over Privacy*," Time Magazine*. 13 April 2010: http:// www.time.com/time/world/article/0,8599,1981524,00.html Matthias Kremp, "Courting controversy: Google Prepares Street View Launch in Germany," *Der Spiegel*. 10 August 2010, available at http://www.spiegel.de/international/germany/courting-controversy-google-prepares-streetview-launch-in-germany-a-711090.html. Kevin O'Brien, "Many Germans Opt out of Google's Street View." *The New York Times*. For the court decision, see "Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void," *Federal Constitutional Court Press Office*. 27 February 2008, available at http://www.bundesverfassungsgericht.de/en/press/bvg08-022en.html

[29] For background on the German court case, see "The World from Berlin: Germany's New Right to Online Privacy," *Der Spiegel*. 28 February 2008, available at http://www.spiegel.de/international/germany/the-world-from-berlingermany-s-new-right-to-online-privacy-a-538378.html.

[30] Patrick Donahue, "Germany says US spying requires serious discussion" Bloomberg, 28 February 2014, available at http://www.bloomberg.com/news/2014-02-27/germany-says-u-s-spying-requires-serious-discussion.html.

[31] David E. Sanger, "U.S. and Germany Fail to Reach a Deal on Spying," *The New York Times*, 1 May 2014, available at

number of potential forms.[32] Most notably, Chancellor Merkel has suggested that Europe should build out its own Internet infrastructure, permitting Germany to keep its data within Europe. In support of this suggestion, Markel declared that, "European providers [could] offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic."[33]

What such a proposal would mean in practice is unclear; what is clear, however, is that some Germany technology companies are now spearheading the data localization movement. In particular, Deutsche Telekom, the largest provider of high-speed Internet and wireless services in Germany and the largest telecommunications organization in the European Union, has begun to act in advance of any German government legislation. In partnership with GMX, one of Germany's largest email providers, the company has already implemented its "e-mail made in Germany" service, a program that promises to keep German email communications within German territory.[34] Thomas Tschersich, who heads Deutsche Telekom's IT Security, explained that IP addresses will be used to recognize when both the sender and the recipient of the emails are in Germany, and based on that information, arrangements between national email providers will be used to transfer this information.[35]

Further, consistent with, and supported by, Chancellor Merkel's declarations of Internet independence, Deutsche Telekom has also raised the idea of creating a "Schengen area routing," a network for the 26 European countries that have agreed to remove passport controls at their borders.[36] (The Schengen area does not include the U.K., which the Snowden documents have

---

http://www.nytimes.com/2014/05/02/world/europe/us-and-germany-fail-to-reach-a-deal-on-spying.html?partner=rss&emc=rss&smid=tw-thecaucus&_r=0

[32] "Germany looks to erect IT barrier," *Deutsche Welle*, 4 November 2013, Available at http://www.dw.de/germany-looks-to-erect-it-barrier/a-17203480.

[33] Alison Smale, "Merkel Backs Plan to Keep European Data in Europe" *The New York Times*, 16 February 2014, available at http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html?hp&_r=0.

[34] Amar Toor, "Brazil and Germany make moves to protection online privacy, but experts see a troubling trend towards Balkanization." *The Verge*, 8 November 2013, available at http://www.theverge.com/2013/11/8/5080554/nsa-backlash-brazil-germany-raises-fears-of-internet-balkanization.

[35] Chiponda Chimbelu, "No welcome for Deutsche Telekom national Internet plans from EU Commission." *Deutsche Welle,* 11 November 2013, available at http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111. Michael Birnbaum, "Germany looks at keeping its Internet, email, traffic inside its borders." *The Washington Post*, 31 October 2013, available at http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html.

[36] Alison Smale, "Merkel Backs Plan to Keep European Data in Europe." *The New York Times*, 16 February 2014, available at http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html?hp&_r=0.

revealed has closely cooperated with the U.S. spying programs through its own signals intelligence agency, the GCHQ). This network would supposedly allow the network nations' citizens securely to exchange data within the area without having to send that data to the United States. "The idea is that when the sender and recipient of any Internet data are in Germany their data is not sent via another country, as it sometimes is today," Philipp Blank, a Deutsche Telekom spokesman explained. Blank left no doubt as to which other countries' practices—and companies—troubled him: "We're simply asking: Why does an e-mail from Bonn to Berlin have to pass through New York or London?"[37]

The role of the German government in facilitating data localization proposals is currently being hotly debated within Europe, and between Germans and Americans. The U.S. Trade Representative**,** among other U.S. government officials, is advocating strongly that Europe not move forward with the idea of EU network services that bar data from crossing the Atlantic, arguing (as this paper argues) that it would be unwise, uneconomical, and counterproductive.[38] But as of the time of this writing, these proposals are still under serious consideration.

Quick Glance: South Korea's Financial Services Requirement

The South Korean Financial Services Commission is considering regulations that would require insurers and other financial institutions to maintain servers for housing company financial data in-country, and would restrict transfers of such data outside of South Korea's borders. The U.S.-Korea Free Trade Agreement (KORUS FTA) states, "Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders," and establishes principles for non-discrimination for digital products.[39] However, this provision is a non-binding feature of the FTA, and could[40] be revoked by the Korean Parliament. Revocation would create a daunting logistical obligation for American financial firms and the companies those firms use to store their data.

B. *The European Union and the U.S.-EU Safe Harbor Agreement*

Germany's data localization movement is complicated by the fact that German Internet law is deeply integrated within the broader legal framework of the European Union, which itself is in the midst of a lengthy process of debate regarding a new General Data Protection Regulation ("GDPR"), a process that

[37] Luisa Schaeter (interviewer), "Deusche Telekon: Internet data made in Germany should stay in Germany," *Deutsche Welle*, 18 October 2013, available at http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891.
[38] Richard Chirgwin, "USA opposes Schengen cloud Eurocenric routing plan," *The Register,* 7 April 2014, available at http://www.theregister.co.uk/2014/04/07/keeping_data_away_from_the_us_not_on_ustr/.
[39] U.S.-Korea Free Trade Agreement, chapter 15.
[40] ITIF (2013), Ibid.

has been underway since 2012. As in Germany, the reaction to the Snowden revelations within other member states of the EU was overwhelmingly critical. "There's real anxiety among consumers about how their data could be used fraudulently or without their knowledge," said Vincent Carre, who heads Orange's data-privacy unit. He then revealed what may be his principal interest in emphasizing this anxiety: "[European companies] are in a great position to reassure customers."[41]

Following the first of Snowden's releases, the European Parliament adopted a non-binding resolution that condemned the U.S. spying and called for Europe to respect "democratic, judicial and parliamentary safeguards and oversight in a digital society."[42] That resolution was soon followed by another, threatening to suspend law enforcement and intelligence agreements between Europe and the U.S.[43] While that threat was never carried out, and may have been largely symbolic and directed principally at the Parliament Members' electorates, the EU has more significantly been moving forward with a range of Internet and data policy proposals, some of which could lead to data localization, even if they are not explicitly worded to do so. With total U.S. exports of digital services, including cloud-computing services, to Europe estimated at $162 billion per year,[44] these new data rules are being closely monitored by the U.S. tech industry.

The EU and the U.S. have long taken different approaches to privacy and data protection governance and enforcement.[45] Under the 1995 EU Privacy Directive, organizations may only transfer personally identifiable information from the EU to countries that the European Commission has deemed to have adequate data protection laws; crucially, the U.S. has not been classified as one of those countries. In the United States, lawmakers have historically relied largely on industry self-regulation rather than law, in line with American

---

[41] Cornelius Rahn and Marie Mawad, "Zuckerberg's Data Stance Faces Privacy Backlash in Europe," *Bloomberg*, 20 February 2014, available at http://www.bloomberg.com/news/2014-02-21/zuckerberg-s-data-stance-faces-privacy-backlash-in-europe.html.

[42] "EP draft report condemns Internet surveillance." *Neurope*, 10 January 2014, available at http://www.neurope.eu/article/ep-draft-report-condemns-internet-surveillance.

[43] "European Parliament resolution of 4 July 2013 on the US National Security Agency surveillance programme surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP))," 4 July 2013, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN.

[44] Jessica R. Nicholson and Ryan Noonan, "Digital Economy and Cross Border Trade: The Value of Digital-Deliverable Services," ESA Issue Brief 01-14*, US Department of Commerce, Economics and Statistics Administration*, 27 January 2014, available at http://www.esa.doc.gov/sites/default/files/reports/documents/digitaleconomyandtrade2014-1-27final.pdf.

[45] For a useful discussion of the history and divergent philosophies, see "U.S. Commerce Department General Counsel Cameron F. Kerry Keynote Address at the German Marshall Fund of the United States," 28 April 2013, available at http://www.commerce.gov/news/speech/2013/08/28/us-commerce-department-general-counsel-cameron-f-kerry-keynote-address-german.

laissez-faire principles and the long-argued assertion from industry leaders that onerous regulations constitute a hindrance to technical innovation and free competition. In order to mitigate the effects of these differences on commerce and trade, in 2001 the U.S. and EU agreed to a "Safe Harbor" framework by which companies subject to American law and European companies transferring or processing data in the U.S. were both safe from European litigation as long as they adhered to certain basic privacy principles set forth in the Directive.[46] Under this system, U.S. firms may self-certify that they meet the requirements of the Directive, allowing them to qualify at the corporate level, even though the United States does not qualify at the national level.[47]

The continued viability of the safe harbor agreement is uncertain, as many European politicians now seem to have concluded that the current arrangement is no longer adequate. In March 2014, less than a year after Snowden began releasing his stolen NSA documents, the European Parliament took a step towards a new set of data security measures intended to strengthen and expand the protections of the Privacy Directive.[48] The new rules, known as the General Data Protection Regulation (which had been under discussion since 2012, but have since Snowden taken on new life and more vigorous requirements) aim to give European Union's 250 million Internet users more say about who gets access to their personal data, and to replace the hodgepodge of privacy rules across the 28 European Union member states with a single body of law, giving businesses and citizens greater certainty about their rights and responsibilities. The European Parliament's commitment to adding force to the Privacy Directive appears to be earnest and likely, although to become law the measure

---

[46] For more information on the Directive, see Jonah Force Hill, "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers." Paper, *Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School*, May 2012, available at http://belfercenter.hks.harvard.edu/publication/22040/internet_fragmentation.html?breadcrumb=%2Fpublication%2F17613%2Fgovernance_and_information_technology.

[47] There are several other legal mechanisms by in which a U.S. firm may transfer data to Europe and vice-versa and satisfy EU privacy laws. These include "Binding Corporate Rules," a process by which firms may define and submit their global policies for certification by EU national authorities, and Model Contracts and Clauses under which the European Commission can decide on the basis of Article 26 (4) of directive 95/46/EC that standard contractual clauses "provide adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals as regards the exercise of the corresponding rights." For details, see "Model Contracts for the transfer of personal data to third countries" available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm and "Overview of Binding Corporate Rules" http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[48] "Progress on EU data protection reform now irreversible following European Parliament vote" European Commission - Memo/14/186 European Commission, 12 March 2014, available at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

will also have to be adopted by the Council of Ministers using the famously tricky-to-navigate co-decision procedure.[49]

New rules would include much higher fines for firms deemed to be in violation of data protection law in the EU (including those firms located outside of Europe), a limited right of citizens to demand the deletion or limited retention of their personal data, and strict limitations on what can be done with EU citizens' data outside the Union. Fines for violating certain rules could be as high as €100 million or up to five percent of an enterprise's annual revenue, whichever is larger[50]—an eye-popping sum. Companies such as Google could, under the new EU regulatory regime, face much higher fines for privacy breaches than the relatively trivial sums they pay today for the same violation. Perhaps most importantly, EU privacy rules now apply to the processing of EU citizens' data, even if that data is processed in another country, a requirement that could force U.S. firms to set up additional servers in Europe.

The effect of these proposed EU rules could seriously undermine the position of some U.S. firms. They would bar some firms' practice, embedded in their business models, of selling data (not necessarily sensitive or private data) to third parties, while others use data analytic tools at odds with the new rules. Furthermore, business models aside, the rules if adopted may require U.S. firms to place their servers, and European citizen data they hold, permanently in Europe, potentially a prohibitively expensive—or even technically unfeasible—requirement. The consequences, in either case, would be *de facto*, if not *de jure*, data localization.

---

[49] For a flowchart of the co-decision system, see http://ec.europa.eu/codecision/stepbystep/diagram_en.htm.

[50] Memo/14/186, Ibid.

Quick Glance: Russia's "Six-Month" Local Server Law

In April 2014, Russia's State Duma approved a draft law[51] that would require Internet companies such as Google to locate servers handling Russian traffic inside the country and store user data locally for six months after the data is created.[52] The move came as Russian agencies had been pressuring foreign Internet companies for data on Ukrainians who had been supporting the February overthrow of the country's Kremlin-backed president, Viktor Yanukovych, and following President Vladimir Putin's remarks that the Snowden disclosures had demonstrated that the Internet was a "CIA project."[53] How the law will be enforced remains unclear, but the draft includes an ambitious note about jurisdictional scope: "In the event that the communication service organizer is located beyond the borders of the Russian Federation," it reads, "but the *user* of the services is located within Russian territory, the location of services rendered is the territory of the Russian Federation."[54] Thus, as is often the case with localization proposals in other countries, the new law could have the effect of forcing non-Russian firms and their services out of the country.

C. *Brazil and the "Marco Civil da Internet"*

In certain interesting ways, the Brazilian response to the Snowden revelations has mirrored that of Germany. Brazilians, like their German counterparts, took serious umbrage when they learned that the NSA targeted their head of state—in Brazil's case, President Dilma Rousseff. Perhaps more significantly, if less sensationally, Brazilians were angered to learn that the NSA conducted a program that infiltrated the networks of Brazil's national oil and gas company, Petrobas.[55]

---

[51] "On Amending the Federal Law "On Information, Information Technologies and Protection of Information" and Certain Legislative Acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks" (translated using Google Translate), available at http://asozd2.duma.gov.ru/main.nsf/(SpravkaNew)?OpenAgent&RN=428884-6&02

[52] Ilya Khrennikov and Anastasia Ustinova, "Putin's Next Invasion? The Russian Web," *Bloomberg BusinessWeek*, 1 May 2014, available at http://www.businessweek.com/articles/2014-05-01/russia-moves-toward-china-style-internet-censorship.

[53] Ewen MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup," The Guardian, 24 April 2014, available at http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

[54] Kevin Rothrack, "Russia's Parliament Prepares New "Anti-Terrorist" Laws for Internet." Global Voices, 16 January 2014, available at http://advocacy.globalvoicesonline.org/2014/01/16/russias-parliament-prepares-new-anti-terrorist-laws-for-internet-censorship-putin/

[55] "NSA Documents Show United States Spied Brazilian Oil Giant (*sic*)," *Globo/Fantastico*, 8 September 2013, available at http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html.

The parallels between Brazil and Germany have not been lost on the leaders of either of the two countries. Brazil, like Germany, is deeply scarred by its own history of military dictatorship and the system of state surveillance orchestrated by that regime. When the NSA leaks became public, President Rousseff, who herself fought against Brazil's dictatorship as an anti-government guerilla fighter, canceled a planned U.S. visit and state dinner with President Obama.[56] Later, in November, she launched a long and impassioned diatribe from the podium of the UN General Assembly against the intrusion of U.S. surveillance.[57] Acting upon their shared perceptions of the seriousness of the NSA's transgressions, Germany and Brazil have jointly proposed a resolution on online privacy to the UN,[58] and have put forward proposals to build an undersea fiber-optic cable that is intended to funnel Internet traffic between South America and Europe, without having to pass through the U.S.[59]

On the home front, the Brazilian government has announced plans to abandon Microsoft Outlook for its own domestic email system that utilizes only Brazilian data centers.[60] The Brazilian parliament has also recently passed its "Marco Civil da Internet," an Internet "bill of rights"—the first major Internet policy legislation in Brazilian history—that enshrines fundamental rights for Internet users, and establishes legal obligations of Internet companies in furtherance of those rights. The Brazilian Parliament and ministries have, since 2009, been engaged in negotiations over the details of the bill, which the Center for Democracy and Technology, a prominent American technology think tank, has called a "major victory for Brazilian civil society," in that it provides sweeping new protections for Brazilian Internet users.[61]

Following the Snowden firestorm, however, some legislators proposed to expand the Marco Civil beyond its "bill of rights" function, arguing for the inclusion of a provision requiring foreign companies to store copies of all data pertaining to Brazilians in local data servers. That provision, which was initially backed by President Rousseff but has since been removed from the

---

[56] "Brazil's Rousseff cancels state visit to U.S. over spying report," *Reuters*, 17 September 2013, available at http://www.reuters.com/article/2013/09/17/usa-security-snowden-brazil-idUSL2N0HD13S20130917.

[57] Julian Borger, "Brazil president: US surveillance a breach of international law," *The Guardian*, 24 September 2013, available at http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

[58] "Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms" United Nations draft resolution of Brazil and Germany. 1 November 2013, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45

[59] Robin Emmott, "Brazil, Europe plan undersea cable to skirt US spying." *Reuters*, 24 February 2014, available at http://www.reuters.com/article/2014/02/24/us-eu-brazil-idUSBREA1N0PL20140224.

[60] Claire Cain Miller, Ibid.

[61] Emily Barabas, "Brazil's Internet Bill of Rights Regains Momentum in Congress," *Center for Democracy and Technology, Global Internet Policy*, 27 March 2014, available at https://cdt.org/brazils-internet-bill-of-rights-regains-momentum-in-congress/

current bill as passed,[62] was aimed at enabling greater access for Brazilian law enforcement to data stored abroad or belonging to foreign companies.[63]

While the Marco Civil was signed into law on April 23, 2014[64] with the most potent localization provision rescinded, one provision remained, Article 11,[65] which deeply troubles international business interests, in that it extends the reach of Brazilian law to any Internet service in the world with Brazilian users. A firm based in the United States whose services are used by Brazilians could, for example, be penalized for adhering to its domestic data-disclosure laws if they conflict with Brazil's. Penalties include fines of up to ten percent of a firm's Brazilian revenues or even termination of the offending company's services in Brazil.[66] Additionally, immediately following the passage the Marco Civil, Brazil's largest paper, *Folha de Sao Paulo*, reported that the Minister of Communications, Paulo Bernardo, stated that the government has not totally abandoned its desire to pursue a local server requirement, despite the deletion of the provision from the Marco Civil, and is considering pursuing the policy as part of a new "Data Protection Law."[67]

---

[62] Paulo Trevisani and Loretta Chao, "Brazil lawmakers remove controversial provision in Internet bill," *The Wall Street Journal*, 19 March 2014, available at http://online.wsj.com/news/articles/SB10001424052702304026304579449730185773914

[63] Interview with Carolina Rossini, *New America Foundation*, 7 March 2014.

[64] "Brazil enacts Internet Bill of Rights," *The Washington Post*, 23 April 2014, available at http://www.washingtonpost.com/world/the_americas/brazil-passes-bill-on-internet-privacy/2014/04/23/0f5922ca-cae1-11e3-b81a-6fff56bc591e_story.html.

[65] "Art. 11. Any process of collection, storage, custody and treatment of records, personal data or communications by connection providers and Internet applications providers, in which at least one of these acts occurs in the national territory, shall respect Brazilian law, the rights to Privacy, and the confidentiality of personal data, of private communications and records." Portuguese: "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverá ser respeitada a legislação brasileira, os direitos à privacidade, ao sigilo dos dados pessoais, das comunicações privadas e dos registros." Projeto de Lei n. 2126 de 2011 [Draft Law No. 2126 of 2014], translated by Carolina Rossini, Project Director for the Latin America Resource Center at the Internet Governance and Human Rights Program at the New America Foundation's OTI

[66] "The net closes: Brazil's magna carta for the web," *The Economist*, 29 March 2014, available at http://www.economist.com/news/americas/21599781-brazils-magna-carta-web-net-closes.

[67] Bruno Favero, "Governo nao desistiu de data centers no Brasil, diz Paulo Bernardo,' *Folha de S. Paulo*, 23 April 2014 (translated using Google with assistance from Portuguese speakers), available at http://www1.folha.uol.com.br/tec/2014/04/1444381-governo-nao-desistiu-de-data-centers-no-brasil-diz-paulo-bernardo.shtml; Flavia Foreque, "Governo nao vai insister em data centers no Brasil, afirma Dilma," *Folha de S. Paulo*, 24 April 2014, (translated using Google with assistance from Portuguese speakers) available at http://www1.folha.uol.com.br/poder/2014/04/1444753-governo-nao-vai-insistir-em-data-centers-no-brasil-afirma-dilma.shtml.

With more than 94 million Internet users, and Facebook usage second only to the United States,[68] the Brazilian market is enormously important for the major U.S. Internet companies. It will be extremely difficult and expensive for them to remove themselves from the Brazilian market. However, if the Brazilian President elects aggressively to enforce the rules found in the Marco Civil, or if the Brazilian government pursues localization as part of other legislation such as a new data protection law, affected U.S. companies may be left with no choice but to take their business elsewhere.

Quick Glance: Indonesia's "Regulation 82"

In Indonesia, U.S. companies are closely watching how a 2012 amendment to the Law No. 11 regarding "Implementation of Electronic Systems and Electronic Transactions ('Regulation 82')" and how "public service" data is defined.[69] According to Regulation 82, all digital providers of a "public service" are required to build a domestic data center in the country. The government has not yet offered a regulatory definition of "public service" under Regulation 82. For the time being, regulators are relying on a definition found in Public Service Law no. 25 of 2009. There, "public service" is defined extraordinarily broadly as "anything that is pertinent to people's welfare." This crucial definitional issue is currently being worked out in the Indonesian legislature and within the Ministry of Communications and Information. Depending on how expansively or narrowly lawmakers ultimately define the term, they could determine how freely American companies will be to operate in Indonesia.

D. *India and the National Security Council*

In September 2013, *The Hindu* newspaper, one of India's largest English language dailies, reported that the NSA had used the PRISM and other secret programs to gather information on India's domestic politics and on a variety of the country's most important strategic and commercial interests, including India's nuclear and space industries.[70] A separate NSA document, also obtained by *The Hindu*, suggested that the NSA had selected the office of India's UN

[68] Carolina Rossini, "Internet and Statecraft: Brazil and the Future of Internet Governance," *New America Foundation*, 2 October 2013, available at http://oti.newamerica.net/blogposts/2013/internet_and_statecraft_brazil_and_the_future_of_internet_governance-93553.

[69] Vanesha Manuturi and Basten Gokkon, "Web giants to build data centers in Indonesia?" *The Jakarta Globe*, 15 January 2014, available at http://www.thejakartaglobe.com/news/web-giants-to-build-data-centers/; Richard Cornwallis, "New Regulation on Electronic Systems and Electronic Transactions" *Mondaq*, 21 February 2013, available at http://www.mondaq.com/x/222132/IT+internet/New+Regulation+on+Electronic+Systems+and+Electronic+Transactions.

[70] Shobhan Saxena, "NSA planted bugs at Indian missions in DC, UN," *The Hindu*, 25 September 2013, available at http://www.thehindu.com/news/international/world/nsa-planted-bugs-at-indian-missions-in-dc-un/article5164944.ece.

mission and Washington embassy as "location targets," where records of Internet traffic, emails, telephone and office conversations could potentially be accessed.[71] Indeed, Snowden's disclosures revealed that India was one of the most highly surveilled countries on the NSA target list.[72]

In contrast to the anger generated by the Snowden revelations within other democratic countries such as Germany and Brazil, and despite the apparent extent of the NSA's targeting of Indian security and political secrets, the Snowden revelations did not evoke wide-scale condemnation in India, nor did a particularly harsh response issue from Delhi, at least initially.[73] After discussing the matter with U.S. Secretary of State John Kerry, India's External Affairs Minister (Foreign Minster) Salman Khurshid (who with the coming of the BJP government has, of course, since been replaced) stated that, "We had an issue, which was discussed when Secretary Kerry was in India… He [Kerry] made a very clear explanation that no content has been sought or received of any email… So, I think as far as we are concerned, there is no issue today."

The reasons for the measured, even mild, initial Indian diplomatic response are complex—perhaps stemming from India's own terrorism concerns[74]—but it seems possible that at the level of Internet policy, as opposed to bilateral or international relations, a more forceful response may be coming, and it may take the form of domestic data localization laws. The Indian national security establishment, at least, appears to be considering localization in the wake of Snowden's revelations as an important policy objective. Significantly, in February 2014 *The Hindu* published the contents of an internal memorandum of the Indian National Security Council (NSC) proposing a policy that would require Indian data to be stored locally.[75] According to the memorandum, the policy would provide that "[a]ll email service providers may be mandated to host servers for their India operations in India.[76] All data generated from within India should be hosted in these India-based servers and this would make them

---

[71] Saxena, Ibid.

[72] Glenn Greenwald and Shobhan Saxena, "India among top targets of spying by NSA," *The Hindu*, 23 September 2013, available at http://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece.

[73] Brindaalakshmi K, "Supreme Court to Hear PIL Against NSA Surveillance of Indian Data," *Medianama*, 26 June 2013, available at http://www.medianama.com/2013/06/223-supreme-court-to-hear-pil-against-nsa-surveillance-of-indian-data-report/.

[74] In explaining India's tempered response to the Snowden disclosures revealing that the country had been one of the most intensely surveilled by the NSA, Indian External Affairs Minister Salman Khurshid acknowledged that, "some of the information they [the U.S.] got out of their scrutiny, they were able to use it to prevent serious terrorist attacks in several countries." "It is not actually snooping: Khurshid on US surveillance," *The Hindu*, 2 July 2013, available at http://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece

[75] Thomas K. Thomas, "National Security Council proposes 3-pronged plan to protect Internet users," *The Hindu*, 13 February 2014, available at http://www.thehindubusinessline.com/features/smartbuy/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece.

[76] Thomas, Ibid.

subject to Indian laws."[77] The NSC proposal would prohibit "as a general principle, mirroring of data in these servers to main servers abroad."[78] Additionally, India's National Security Advisor has called on the Department of Telecom to mandate that all telecom and Internet companies route local data through the National Internet Exchange of India (NIXI) to ensure that domestic Internet traffic remains within the country, and "to limit the capacity of foreign elements to scrutinize intra-India traffic."[79]

This latest proposal by the NSC is, at this point, only a recommendation. It may not gain momentum. But U.S. companies have already been on shaky footing in India for the past several years. Indeed, 22 of the largest and most prominent U.S. tech firms had already been ensnared in a series of controversies—most importantly for their failure or unwillingness to remove selected "objectionable" and inflammatory content that had been hosted through their services—that have seriously threatened their business prospects in the country.[80] A localization proposal of the kind suggested by the NSC might find further support among those parties already dissatisfied with the American firms' that seem to place a higher premium on Anglo-American notions of freedom of expression than on deeply-held Indian social and cultural preferences.

The formation of a government under the leadership of the Bharatiya Janata Party (BJP)—which came to power in the Indian national elections in May 2014—is likely to give greater impetus to Indian localization efforts. During the campaign, BJP leaders stated publicly that data localization might be a necessary means to force foreign (read: American) Internet companies to comply with local law and to respect Indian cultural norms.[81] Moreover, it was revealed in June 2014 that the NSA had been intercepting the communications of senior BJP party members—likely including Prime Minster Narendra Modi—in the years prior to the BJP's election victory in 2014. The reaction from the BJP government, in contrast to its Congress Party predecessor, was far less tepid. The U.S. ambassador was immediately summoned for consultation; Syed Akbaruddin, a spokesman for the Indian Foreign Ministry, lamented that the episode was "extremely disconcerting." This contretemps and the apparent

---

[77] Thomas, Ibid.
[78] Thomas, Ibid.
[79] Thomas K Thomas, "Route domestic net traffic via India servers, NSA tells operators," *The Hindu*, 14 August 2014, available at http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece.
[80] Jonah Force Hill, "India's Internet Freedom Nightmare," *The Diplomat*, July 2012, Available at http://thediplomat.com/2012/08/indias-internet-freedom-nightmare/1/. Jonah Force Hill, "India: the new front line in the global war for Internet freedom," The Atlantic, June 2012 http://www.theatlantic.com/international/archive/2012/06/india-the-new-front-line-in-the-global-struggle-for-internet-freedom/258237/.
[81] Indu Nandakumar and Neha Alaadhi, "BJP plans to lure Facebook, Google, Yahoo if it comes to power," *Economic Times*, available at http://economictimes.indiatimes.com/news/politics-and-nation/bjp-plans-to-lure-facebook-google-yahoo-if-it-comes-to-power/articleshow/34131445.cms.

deterioration of the U.S.-India relationship may have little direct bearing on the localization issue. But is clear that Indian government opposition to data localization policies (at least with regards concerns that attempts at localization rules could adversely impact US-India relations) may be at an all time nadir.[82]

India has become an important outsourcing hub for U.S. multinational organizations. American firms have established extensive IT and back-office centers in India's growing technology capitals, such as Bangalore and Hyderabad. The total expulsion of American tech firms from the country seems remote,[83] but any significant data localization legislation of the kind proposed by the NSC could impose a substantial financial burden on American companies; perhaps more importantly, it could jeopardize the firms' business prospects in a country in which reside hundreds of millions of potential customers.

IV. DIVERSE MOTIVATIONS

Upon first glance, the preceding case studies present a consistent narrative: for the nations now considering localization for data, the Snowden revelations exposed an NSA that had overstepped the boundaries of acceptable surveillance, violated citizen privacy, and catalyzed public and government opinion in favor of forceful action in response. For policymakers, data localization offers a seemingly simple and effective solution. Under closer examination, however, a more complicated picture emerges. The localization movement is in fact a complex and multilayered phenomenon, with the objective not only—or even primarily—of protecting privacy. Depending on the country in which it is being advanced, localization also serves to protect domestic businesses from foreign competition, to support domestic intelligence and law enforcement ambitions, to suppress dissent and to stir up populist enthusiasms for narrow political ends. Direct evidence of these other objectives for which privacy seems to be a pretext is by its nature difficult to uncover: rarely to policy-makers admit to seeking protectionist goals, to spying on their populations, to suppressing dissent or to exploiting populist emotions. Yet, by viewing the localization movement in the context of other state and corporate interests and activities, it is possible to uncover these other, less exalted ends.

---

[82] Whitney Eulich,"India recoils at reported NSA spying on its Hindu nationalist party," Christian Science Monitor, 2 July 2014, available at http://www.csmonitor.com/World/Security-Watch/terrorism-security/2014/0702/India-recoils-at-reported-NSA-spying-on-its-Hindu-nationalist-party

[83] It is worth noting that following Snowden, the Indian government is considering restricting its employees' use of certain Google services following Snowden. See Indu Nandakuman and J. Srikant, "Cyber-spying fallout: Govt may restrict usage of Google's Gmail for employees," *Economic Times*, 30 August 2013, available at http://articles.economictimes.indiatimes.com/2013-08-30/news/41618948_1_google-india-us-national-security-agency-government.

A. *Protectionism*

Powerful business interests undoubtedly see data localization as an effective and convenient strategy for gaining a competitive advantage in domestic IT markets long dominated by U.S. tech firms. To localization proponents of this stripe, the NSA programs serve as a powerful and politically expedient excuse to pursue policies protective of domestic businesses.

As an illustration, data localization in Germany presents clear economic benefits for a most powerful industry advocate for localization, Deutsche Telekom (DT). Whether by way of its "email made in Germany" system or the Schengen area routing arrangement, DT looks poised to gain from efforts to reduce the prominence of American tech firms in Europe. It is no wonder that the company has been spearheading many of the localization proposals in that country. As telecommunications law expert Susan Crawford has noted, DT has been seeking to expand its cloud computing services for years, but has found its efforts to appeal to German consumers stifled by competition from Google and other American firms.[84] T-Systems International GmbH, DT's 29,000-employee distribution arm for information-technology solutions, has been steadily losing money as a result.[85] Moreover, Crawford suggests that DT would not be content with gaining a greater share of the German market; she points out that through a Schengen routing scheme, "Deutsche Telekom undoubtedly thinks that it will be able to collect fees from network operators in other countries that want their customers' data to reach Deutsche Telekom's customers."[86]

Similarly, companies and their allies in government in Brazil and India look to profit from data localization proposals. Indeed, the governments of both nations have for years sought to cultivate their own domestic information technology sectors, at times by protecting homegrown industries with import tariffs and preferential taxation. Brazilian President Rousseff has on numerous occasions stated that her government intends to make Brazil a regional technology and innovation leader; in recent years the government has proposed measures to increase domestic Internet bandwidth production, expand international Internet connectivity, encourage domestic content production, and promote the use of domestically produced network equipment.[87] India, more controversially, has at times required foreign corporations to enter into joint ventures to sell e-commerce products, and has compelled foreign companies to

---

[84] Susan Crawford, "NSA scandal may help build cyber barriers," *Bloomberg*, 27 December 2013, available at http://www.bloombergview.com/articles/2013-12-27/nsa-scandal-may-help-build-cyber-barriers.

[85] Crawford, Ibid

[86] As things stand today, non-German networks often seek to avoid sending data through Deutsche Telekom's wires when routing Internet traffic to German customers because that company often refuses to exchange traffic on a no-payment basis, as is often customary for so-called "backbone" providers. Crawford, Ibid.

[87] Bill Woodcock, "On Internet, Brazil is Beating Us at Its Own Game," *Al Jazzera America*, 20 September 2013, available at http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html

transfer proprietary technology to domestic firms after a predetermined amount of time.[88] It should thus come as no surprised that the Internet Service Providers Association of India, India's largest Internet industry group, was one of the first organizations to lobby for national localization policies following the Snowden disclosures.[89]

Brazil and India are, of course, not alone in this respect. Indonesian firms are constructing domestic cloud service facilities with the help of government grants,[90] while Korea is offering similar support to its own firms.[91] For the governments and corporations of these nations, long frustrated by their inability to develop a domestic IT industry that can compete on an even playing field with the U.S. technology giants, data localization is one means to confront, and perhaps overcome, the American Internet hegemony.

B. *Domestic Surveillance and Law Enforcement*

Just as protectionist purposes can be advanced by data localization, so too can the objectives of domestic intelligence and law enforcement agencies. Initially, we know that governments already are engaged in sophisticated surveillance of their own populations. For example, despite the German government's vitriolic public protestations over NSA spying, Germany itself maintains a fairly robust intelligence collection program, a program that has been growing over the past few years.[92] According to the German newsweekly *Der Spiegel*, the BND, the rough German equivalent of the American NSA, maintains secret arrangements with German telecommunications and Internet firms in order to provide the German spy agency with direct access to data flowing over domestic fiberoptic cables.[93] The agency has also reportedly installed "taps" on Germany's largest Internet exchange point in Frankfurt, known as the DE-CIX, in a manner consistent with the NSA's tactics.[94] India, which also maintains its own sizeable

---

[88] Department of Telecommunications Order No. 10-15/2009-AS-III/193 cited in Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, Ibid.

[89] Thomas K. Thomas, "Indian Net firms want Google, Facebook to go local," The Hindu Business Line, 8 June 2013, available at: http://www.thehindubusinessline.com/industry-and-economy/info-tech/indian-net-firms-want-google-facebook-to-go-local/article4795367.ece.

[90] Efi Nurfiyasari, "Multipolar Technology Puts $100m into Data Center," *Jakarta Globe*, 9 July 2013, available at http://www.thejakartaglobe.com/business/multipolar-technology-puts-100m-into-data-center/.

[91] "Cloud Computing Market in Korea 2014-2018" *Research and Markets Report*, December 2013, http://www.researchandmarkets.com/research/q3gd5q/cloud_computing

[92] Ian Steadman, "German spy agency gets funding boost to aid web traffic interceptions," *Wired*, 17 June 2013, available at http://www.wired.co.uk/news/archive/2013-06/17/german-spy-power-increase

[93] "The German Prism: Berlin wants to spy too," *Der Spiegel*, 17 June 2013, available at http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html.

[94] Archibald Preuschat and Anton Trolanovski, "German intelligence admits Frankfurt email tap," *The Wall Street Journal*, 9 October 2013, available at http://blogs.wsj.com/digits/2013/10/09/german-intelligence-admits-to-frankfurt-e-mail-tap/

intelligence community,[95] is likewise in the process of beefing up its signals intelligence capabilities, importantly its Centralized Monitoring System (CMS), a massive nation-wide intelligence collection program which is expected to give the Indian government enormous powers to access phone conversations, video conferences, text messages, and emails, in real time, with minimal court oversight.[96]

If a government already has a sophisticated communications surveillance capacity, it would not be surprising that that it would want to enhance that capacity—certainly, that is what the United States has done. It would seem naïve to suppose that other governments would act differently. Data localization in both German and India and elsewhere, would offer just such enhancement, through two important intelligence functions. First, it allows domestic intelligence agencies to better monitor domestic data by either forcing data to be stored in local servers (indeed, India has previously required two international firms, Research in Motion, Nokia, Google, and Skype to locate servers and data domestically[97] for intelligence collection purposes), or by requiring that data to be held by local firms over which domestic intelligence and law enforcement agencies may have greater coercive power. Second, in light of the often-overlooked fact that many intelligence services, such as the BND, cooperate with the NSA in a variety of information sharing programs,[98] governments may view localization as a tactic to gain additional bargaining power with the NSA in negotiations over how much information the American spy agency will share.[99]

See also, Markus Beckehahi, "YES, WE SCAN! Salvaging Public Trust in a Post Snowden Germany." *Stakes are high: Essays on Brazil and the Future of the Global Internet*, a collaboration between the Center for Global Communication Studies, the Internet Policy Observatory, and the Annenberg School for Communications at the University of Pennsylvania, April 2014, Available at http://globalnetpolicy.org/wp-content/uploads/2014/04/StakesAreHigh_BrazilNETmundial_final.pdf#markusbeckedah.

[95] Leslie D'Monte and Joji Thomas Philip, "How the worlds largest democracy is preparing to snoop on its citizens," *Live Mint and The Wall Street Journal*, 3 July 2013, available at http://www.livemint.com/Politics/pR5zc8hCD1sn3NWQwa7cQJ/The-new-surveillance-state.html.

[96] Anurag Kotoky, "India sets up elaborate system to tap phone calls, email," *Reuters*, 20 June 2013, available at http://in.reuters.com/article/2013/06/20/india-surveillance-idINL3N0EV1WT20130620?_ga=1.34122401.1629689602.1397189573.

[97] "Big Brother Must Not Overstep the Limits," *Tehelka*, 3 March 2012, available at http://www.tehelka.com/big-brother-must-not-overstep-the-limits/; Bibhudatta Pradhan and Ketaki Gokhale, "India Asks RIM, Google, Skype to Set Up Local Servers," Bloomberg, 1 September 2010, available at http://www.bloomberg.com/news/2010-09-01/india-asks-rim-google-skype-to-set-up-local-servers-update1-.html

[98] "Indispensible Exchange: Germany Cooperates Closely with the NSA," *Der Spiegel*, 8 July 2013, available at http://www.spiegel.de/international/world/spiegel-reveals-cooperation-between-nsa-and-german-bnd-a-909954.html.

[99] For an excellent account of the ways in which European governments are condemning NSA spying while simultaneously engaging in their own intelligence collection activities, including on their own citizens, see the Congressional testimony of Stewart A. Baker before the Permanent Select Committee on Intelligence, United States House of Representatives,

Moreover, domestic law enforcement agencies (to the extent that, in most democratic countries, law enforcement is administratively and actually separate from intelligence services) surely have reason to view data localization as a potentially valuable evidence-gathering tool, useful in identifying and then prosecuting conventional criminal activities. In connection with investigations and prosecutions, foreign law enforcement often complain that the process by which they request data from U.S. firms (the rules of which are generally negotiated between the United States and foreign governments and then ratified in a Mutual Legal Assistance Treaty) is slow and cumbersome, and that American firms and the U.S. Justice Department are too often uncooperative. The President's Review Group on Intelligence and Communication Technologies estimated that the average time from request to delivery is 10 months, and sometimes years pass before a response arrives.[100] There is uncertainty about when data can be shared, with whom, and on what terms; and it all happens with very little transparency.[101] This process presents annoying and seemingly unjustified interference to foreign law enforcement officials who want to apprehend criminals. The Brazilian government, for example, has requested information from Google for several pending cases in the Brazilian Supreme Court, but has yet to receive it.[102] Similarly, India has often asked the U.S. to serve summonses upon Google, as well as on Facebook, Twitter, and others, for failing to prevent the dissemination of speech prohibited under Indian Law, but has been rejected due to U.S. civil liberties sensibilities.[103] Data localization, for frustrated and impatient law enforcement agencies and their political allies, looks like a straightforward mechanism to free themselves from some of this bothersome dependence on Americans.

C. *Control of Information and Censorship*

While intelligence and law enforcement agencies in democratic countries may look to localization as a way to perform their jobs more effectively, there are governments that surely have a more sinister reason to favor localization. Political elites in authoritarian states unquestionably see local control of the flow of data as a way to control the content of information that reaches their populations. As was mentioned above, data localization has been used in

---

"Potential Amendments to the Foreign Intelligence Surveillance Act" October 29, 2013, available at http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Baker10292013.pdf.

[100] President's Review Group, Ibid.

[101] For good analysis of U.S. MLAT reform, see *Access*, "MLATS: Making Global Data Request Treaties Work for Human Rights?" https://www.youtube.com/watch?v=kD5aSdN-Wkk and Access MLAT Info Sheet, available at https://mlat.info/app.php/.

[102] Rebecca Blumenstein, "Brazil's Rousseff Pressures U.S. on Data Collection," *The Wall Street Journal*, 25 January 2014, available at http://online.wsj.com/news/articles/SB10001424052702304632204579341183665708524

[103] "MLATS and International Cooperation for Law Enforcement Purposes" Presentation of the Centre for Internet and Society, Bangalore, available at http://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf.

China, Iran, Egypt,[104] and other authoritarian states to ease the technical burdens required to exert control over Internet platforms, such as Facebook, which those governments find to be hosting unwanted political speech, or facilitating political dissent. Yet even the leaders of democratic countries at times have wanted the ability to "shut down" data flows to quell political unrest or to censor "subversive" speech. At the time of this paper's writing (April 2014), for instance, the Turkish government appears to have forced local Internet Service Providers (ISPs) to block access to certain servers hosting Twitter's services, in an attempt to stop the communication channel being used to organize anti-government protests challenging the government of Prime Minister Recep Tayyip Erdogan.[105] This effort seems, for the time being, to have been only partially successful, but had aggressive data localization rules been in place, it is not inconceivable that the protestors' efforts to circumvent the blockage would have been far more problematic.[106]

D. *Populist Politics and Anti-Globalization*

Finally, data localization makes for good old-fashioned populist politics, useful in democratic and authoritarian governments alike. People around the world have been deeply and genuinely unsettled by the Snowden revelations. They see the NSA and the United States generally as engaged in the flagrant and comprehensive violation of their privacy, foreshadowing perhaps an Orwellian future to come.[107] Data localization not only seems to offer a simple response to this American challenge to privacy, simple for politicians to explain and simple for citizens to understand. It also serves as a political repudiation not only of dragnet surveillance generally, but of the American government and the American tech sector that is complicit in that government's misconduct. Anti-Americanism is nothing new, nor is its sometimes-cynical use by politicians. But in the digital age, it has new faces: Google instead of Coca-Cola, and the government employee with a computer rather the soldier with an M-16 rifle. In an environment in which most Germans consider

---

[104] Matt Richtel, "Egypt Cuts Off Most Internet and Cell Service," *The New York Times*, 29 January 2011, available at http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?_r=0 ; Christopher Williams, "How Egypt shut down the Internet," The Telegraph, 28 January 2011, available at http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

[105] Andrea Peterson, "Turkey strengthens Twitter ban, institutes IP level block." *The Washington Post*, 22 March 2014, available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/22/turkey-strengthens-twitter-ban-institutes-ip-level-block/.

[106] Liam Tung, "Turkey's ISPs hijack Google's DNS service, killing bypass for Twitter, Youtube ban," *CSO*, 31 March 2014, available at http://www.cso.com.au/article/541667/turkey_isps_hijack_google_dns_service_killing_bypass_twitter_youtube_ban/.

[107] Dominic Rushe, "NSA surveillance goes beyond Orwell's imagination—Alan Rusbirdger," *The Guardian*, 23 September 2013, available at http://www.theguardian.com/world/2013/sep/23/orwell-nsa-surveillance-alan-rusbridger

Edward Snowden a hero,[108] not a villain, and more than a million Brazilians signed a petition requesting that President Rousseff grant Mr. Snowden asylum,[109] data localization is political gold.

The link between data localization programs and populist politics may also be drawing on a climate of anti-globalization and a desire to move away from a globally integrated, and perhaps American-hegemonic, Internet. Of course, globalization is understood by its critics to be broader than the ambitions of the United States. Nevertheless, it is above all the United States and its enormously powerful companies that represent all that the critics find morally suspect in globalization. And no American companies have an international reach comparable to that of the great tech companies. A cab driver in Rio, a fruit vendor in Cairo or an elementary school teacher in Delhi may have never heard of JP Morgan, but they are likely to encounter Google and Facebook daily. These companies have become the face of American power in the early decades of the Twentieth Century, and however useful they may be in the lives of these people, they are intrusive in a way that no bank can ever be. They, together with the NSA with which they now linked, are seen by millions to be exercising subtle and nefarious power that reaches into every neighborhood and home.

How can foreign governments rein in that power, and seem to respond to popular demands to be protected from these forces from abroad? Data localization schemes may be one response. As I argue below, localization in fact will not accomplish this or most any other desirable objective, but for now anti-globalization provides a forceful political impetus to plans to restrict the reach of those companies.

V. DATA LOCALIZATION: AN UNSOUND POLICY

Whatever mix of purposes constitute the "true" motivations behind the data localization movement, whether domestic industry protectionism, political opportunism, or a genuine—if misplaced—desire for improved data privacy and security, the reality is that data localization, in all of its various forms, creates serious problems without offering many, if any, actual benefits. The problems are manifest not just on a global scale of the efficiency of the Internet, but critically for the specific countries considering the policies. Moreover, some of the localization proposals under consideration—specifically, limitations on data flows to or around specific geographies—would likely require a fundamental restructuring of the Internet's core technical architecture and governance systems, a restructuring that carries with it its own serious drawbacks.

---

[108] "Germans see Snowden as hero but don't favor asylum: poll," *Reuters*, 7 November 2013, available at http://www.reuters.com/article/2013/11/07/us-usa-security-snowden-germany-idUSBRE9A60W920131107.

[109] Rebecca Shabad, "1.1 million petition Brazil to give Snowden asylum," *The Hill*, 14 February 2014, available at http://thehill.com/blogs/global-affairs/americas/198415-group-demands-asylum-for-snowden-in-brazil.

A. *Security and Counter-Surveillance Objectives Are Not Well-Served*

Looking first at data security (the enhancement of which is the ostensible reason for most localization proposals), there is little reason to believe that any of the proposals under consideration would do much, if anything, to mitigate the problems as they have been defined. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Data breaches can and do occur anywhere. Security is instead a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question. Has an Internet service organization put in place comprehensive security policies, and has it routinely audited its software and infrastructure to identify and address security vulnerabilities? These are the useful procedures to protect data. Hence, as a purely technical issue (i.e., irrespective of matters of law and politics), there are few reasons to suspect that a server in Germany will be any safer from attack by those seeking to access information than is a server in the United States, or in Costa Rica for that matter, assuming that they use the same technology and follow the same security procedures.

Advocates for data localization who understand this fact often point to jurisdictional differences between nations as a reason to keep data local. Data stored in the U.S. is unsafe, they argue, because the NSA can obtain it under legal coercion. Data localization (as a restriction on data storage abroad), they insist, would negate this risk. While this may be true in certain respects, the argument omits an important reality, namely that while locating data beyond the borders of the United States might preclude the NSA or FBI from obtaining data via a subpoena or other formal legal mechanism, moving data abroad could actually *empower* the NSA by lowering the legal threshold required to obtain that same data by way *direct intrusion* into foreign data servers or data links. As was mentioned briefly above, U.S. domestic law (as it is currently written and interpreted) puts fairly strict limits on the collection of intelligence information on American soil. Data capture outside the U.S., by contrast, even when that data is in the hands of American firms, is in large measure legally permissible when there is a "national security interest," a fairly broad criterion. Data localization (as a local data requirement) could potentially give the NSA greater freedom to mine data, not less.[110]

---

[110] In addition, by moving data out of the hands of American firms, the NSA would not have to worry about potential blowback from American technology companies like Google, Microsoft, or Yahoo, who, it must be admitted, hold significant influence in Washington and have at their disposal legal teams with a far greater capacity to litigate against the U.S. government than most foreign firms. Other data localization supporters might point to "taps" placed on Internet exchange points and on the links between major server "farms" as a reason to keep servers close and within a national jurisdiction. But as long as intelligence agencies can get physical access to a line, it can be tapped. As historian Norman Polmar, author of *Spy Book: The Encyclopedia of Espionage* has explored, tapping of undersea transmission cables has been a U.S. surveillance tactic for decades. See Olga Khazan, "The creepy longstanding practice of undersea cable tapping," *The Atlantic*, 16 July 2013, available at http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-

Furthermore, while moving data into the servers outside the U.S. may prevent the U.S. government from obtaining certain types of data via subpoena (ignoring the direct intrusion distinction for a moment), data localization in that form would, at the same time, give *domestic* intelligence agencies of the home country increased data collection powers over their citizens' data. Given the fact that it is those domestic agencies and their governments, and not the NSA and the United States, that can more immediately impose and enforce coercive measures upon the citizens, those citizens need to ask themselves, first, which presents the greater threat to their liberty generally, and to the security of their personal information in particular? And, once recognizing that one's own government may not be trusted to abjure obtaining data of its citizens, is a domestic company possessing the data more or less likely than a giant like Google to knuckle under to the demands of one's own government? With respect to most of the nations of the world, where there exist scant judicial independence and little governmental transparency, the questions, I would argue, are answered in the asking.[111]

Ultimately, the only real solution to the kinds of security and surveillance problems brought into the open by the Snowden disclosures lies in international negotiations, agreements, and the development of norms of state behavior. But besides that, what matters is whether or not the organizations hosting the data are protecting that data with the best possible security mechanisms and technology available, and being as transparent as they can be about how they cooperate with intelligence organizations. Accordingly, Internet users should have the freedom to decide which organizations, which companies, are best equipped and able to protect security and offer transparency, whether a Google, an Amazon or a domestic provider. With a number of studies showing that Brazil,[112] Indonesia,[113] and many of the other countries considering localization are among the least well-equipped nations to protect their data, the argument that limiting competition in the market, limiting the options available to firms,

---

standing-practice-of-undersea-cable-tapping/277855/ and cited in: Craig Timberg and Ellen Nakashima, "Agreements with private companies protect U.S. access to cable's data for surveillance," *The Washington Post,* 6 July 2013, available at http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.

[111] Also, it is worth considering that moving data into a potentially less secure non-American firm could give other intelligence agencies, such as those of the Chinese or Russians, added surveillance opportunities.

[112] Ricardo Geromel, "Hackers stole $1b in Brazil, the worst prepared nation to adopt cloud technologies," *Forbes*, 2 March 2012, available at http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/ Carole Theriault, "Brazil's cybercrime evolution—it doesn't look pretty," *Sophos Naked Security*, 5 October 2011, available at http://nakedsecurity.sophos.com/2011/10/05/brazils-cybercrime-evolution-it-doesnt-look-pretty/.

[113] Mark Milian, "Indonesia Passes China to Become Top Source of Cyber-attack Traffic," *Bloomberg*, 15 October 2013, available at http://www.bloomberg.com/news/2013-10-15/indonesia-passes-china-to-become-top-source-of-cyber-attack-traffic.html.

and potentially jettisoning the most security-competent technology companies available would somehow improve security, rather than degrade it, is nonsense.

B. *Economic Growth Objectives Not Well-Served*

Data localization (most especially, as a ban on foreign firms operating local servers) appeals to those political and business leaders who hope to give domestic technology firms a competitive advantage. It also appeals to those leaders who believe that that competitive advantage will, over time, lead to the development of a strong technology sector, following what might be thought of as a "China developmental model," in which early domestic protectionism is tapered off as local firms find their competitive edge. But again, the benefits of this kind of policy (which generally only advantage certain favored local companies) are outweighed by its drawbacks. By prohibiting foreign firms from operating in country, or by making operations prohibitively expensive for foreign firms, governments are dramatically limiting the options available to local consumers. This includes small businesses that often require the cheaper and more advanced services that only international firms can provide. Indeed, even non tech-related industries that nevertheless rely on IT services, such as advanced manufacturing, are likely to see that their costs rise and their efficiencies deteriorate as a consequence of Internet protectionism in the guise of localization.

These costs may not be trivial. The European Centre for International Political Economy has estimated that if and when cross-border data flows between the U.S. and EU are seriously disrupted (assuming existing models for cross-border transfer and processing of data, such as the Safe Harbor and BCRs[114] are disrupted), the negative impact on EU GDP could reach -0.8% to -1.3%, and EU services exports to the United States could drop by as much as -6.7% due to loss of competitiveness.[115] Developing countries, too, would likely suffer. There, Internet access and data services are significant drivers of economic growth. According to several important studies on the issue, access to the Internet can dramatically reduce the effect on developing countries of geographical isolation from major exports markets.[116]And, according to a Deloitte study, expanding access to the 4 billion people who live in developing countries to levels developed economies currently enjoy would increase productivity in those areas by as much as 25 percent, add $2.2 trillion in

---

[114] See *footnote 45* for more on the BCR process.

[115] "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce," European Centre for International Political Economy (commissioned by the U.S. Chamber of Commerce), March 2014, available at https://www.uschamber.com/sites/default/files/legacy/grc/020508_EconomicImportance_Final_Revised_lr.pdf.

[116] See research by Joshua Meltzer, "Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium Sized Enterprises and Developing Countries," Global Economy and Development Working Paper #69, *The Brookings Institution*, February 2014, Available at http://www.brookings.edu/~/media/research/files/papers/2014/02/internet%20international%20trade%20meltzer/02%20international%20trade%20version%202.pdf.

additional GDP, increase the GDP growth rate by 72 percent, add more than 140 million new jobs, and lift 160 million people out of extreme poverty.[117] Certainly, the cost inherent in localization alone will not forestall all of these positive developments, but it would retard them. To leaders in developing nations such as India and Brazil, where data localization measures are under serious consideration, these potential adverse economic impacts ought to give serious pause.

Less directly, but perhaps even more critically as a long-term matter, data localization adversely affects the Internet's capacity for productivity by reducing the Internet's "network effect" and "generativity."[118] By placing limitations on which firms can participate in the network, data localization reduces the overall size of the network, which, according to network theory as well as Metcalfe's Law (which states that the value of a communications network is proportional to the number of users of the system), would bring up both costs and the overall innovative potential of the aggregated network. Consider big data analytics, for example, which often involves the transfer of data from numerous sources without regard to geography and can have major benefits for society.[119] By severing the ties between nations and the data that can be collected an analyzed, data localization vastly diminishes the capacity for new discoveries and for new solutions to some of the world's most pressing problems.

Certainly, there are good reasons for supporting local Internet infrastructure development. Developing local Internet infrastructure has been shown to help to keep costs down (by avoiding having to send data afar unnecessarily and by providing greater options in pricing negotiations) and to keep service available when connectivity to the outside would is disrupted.[120] Governments can and should invest in building up local capabilities. But restricting data flows and preventing foreign competition are not the ways to facilitate that type of local development. Decisions regarding where to store data and how it should be handled—except in the rare cases of national security or other special privacy cases (for example, there may be good reasons for medical data and the like to be given special treatment)—should be driven by efficiencies, not by political expediency.

---

[117] "Value of connectivity: economic and social benefits of expanding Internet access," *Deloitte*, February 2014, available at http://www.deloitte.com/view/en_GB/uk/industries/tmt/extending-internet-access/index.htm.

[118] Zittrain, 2006. Ibid.

[119] Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How Its Changing the Way We Think About the World," Foreign Affairs, May/June 2013, available at http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data?nocache=1.

[120] For background on the issue, see Steve Gibbard, "Geographic Implications of DNS Infrastructure Distribution," The Internet Protocol Journal Volume 10, No. 1, *Cisco*, available at http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_dns-infrastructure.html.

C. *Free Expression & Internet Freedoms Are Not Well-Served*

Most troubling of all the potential harms of data localization is its effect on free expression and Internet freedom. This is ironic, in that to many of its advocates, data localization is a remedy to the threat posed by the NSA to free expression and Internet freedom. I suggest that the opposite is actually true, that the "remedy" only serves to make the danger greater.

The Internet and other online media have become indispensable tools for individuals to communicate globally, and have furthered individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights. Data localization, by centralizing control over digital infrastructure, can diminish this capacity in a number of ways. As was discussed above, data localization as a local server or local data storage requirement can limit freedom by permitting countries more easily to collect information on their citizens (through domestic surveillance). It allows a government more quickly and effectively to shut down Internet services (usually via legal threats to local Internet service providers) that the government believes is abetting unwanted political opposition.[121]

Data localization mandates also can obstruct Internet freedom in other, indirect ways. Restricted routing, in particular, is problematic, because it is not technically possible as the existing Internet is designed or organized. Unlike the telephone network, the Internet operates under a model known as "best effort delivery," where data is delivered to its destination in the most efficient manner possible, without predetermined routes. For instance, data sent from the United States to Botswana will attempt to travel along the shortest and most direct route possible. However, if there is a bottleneck along the shortest route, a packet may find a longer but more expeditious route. This is a core feature of the Internet that makes network congestion easy to navigate around. In order to restrict data routing to specific geographies as governments are advocating, all Internet routers that are currently programmed to follow this "best effort" routing model would have to be reconfigured to prohibit data from one country from moving through the territory of "prohibited" countries. Moreover, since Internet addresses are not always assigned according to a specific geography, the Internet's addressing system currently would have to be dramatically altered as well. Thus, the Border Gateway Protocol (one of the core Internet networking protocols), the Internet's routing tables (the address books by which routers send data), and the process by which IP addresses are allocated, would all have to be modified. Such an undertaking would require a fundamental overhaul not only of the Internet's operating structures, but also of

[121] Granted, there may be legitimate reasons for governments to desire such capabilities: in India, for example, the government faced a nationwide panic, when messages containing images of mutilated bodies began appearing on Indian cell phones, Facebook pages, and Twitter accounts during an episode of communal violence in the country's troubled northeast. For more, see Jonah Force Hill, "India's Internet Freedom Nightmare" *The Diplomat*, August 25, 2012, available at http://thediplomat.com/2012/08/indias-internet-freedom-nightmare/.

the governance structures by which those structures are implemented and standardized.

These are not just arcane concerns of those involved in Internet governance, although they surely are matters that greatly trouble those who favor an efficient and interoperable Internet. These alterations in the way the Internet works will, I believe, materially restrict the power of the Internet to support free expression. These modifications to these core characteristic of the current Internet—modifications that localization would require—may result in intelligence agencies acquiring a previously unavailable capacity to assess where data had originated and where it was heading, because the origin and destination information would be included in the data packet.[122] A centralized governance process, further, which would be required to change the routing protocols and IP allocation system, would give authoritarian countries significantly more influence over how information on the Internet is regulated. In fact, this is one of the main reasons why China, Russia, many Arab states (among others) have pushed for tracked routing protocols in the past,[123] just as they have lobbied for a handover of the global Internet governance system to the U.N.'s International Telecommunications Union.[124]

In short, localization would require dramatic changes to the current structure of the Internet, changes that would have adverse consequences for those who see it as a principal—if not *the* principal—means of global democratization. For some, those adverse consequences would be unintended; more chillingly, there are those who intend precisely those consequences. This would be an enormous price to pay, particularly since the other objectives that are promoted as justifications for localization—namely, security for communications and economic development—are illusory.

VI. RECOMMENDATIONS

Yet despite these many potential problems with data localization—less, rather than more security, less rather than more economic development (particularly among poorer nations), a less integrated and interoperable Internet, and a weakening of the liberating power inherent in the free flow of information—data localization schemes continue on a forward trajectory in several key markets for U.S. technology firms.[125]

---

[122] Interview with Scott Bradner (Harvard University), 28 February 2014.

[123] See coverage of the "ITU Workshop on IP traffic flow measurement" in the ITU-T Study Group 3. 24 March 2011, available at http://www.itu.int/ITU-T/worksem/iptfm/index.html.

[124] Jonah Force Hill, "A U.N. Takeover of the Internet: Existential Threat or Tempest in a Teapot?" *Harvard Kennedy School Technology and Policy Blog*, 9 August 2012, available at http://www.technologyandpolicy.org/2012/08/09/a-u-n-takeover-of-the-internet-existential-threat-or-tempest-in-a-teapot/#.U1x8ufSwKLQ.

[125] Even if data localization as formal policies are not promulgated in the many countries considering them, American companies will still find that many customers have lost faith in their ability to maintain privacy or to resist the demands of the NSA. Indeed, a March 2014 survey by NTT Communications of over 1000 "IT decision-makers" found that nearly nine

Reversing this trend presents a substantial challenge for American companies and the American government. I have offered, below, specific recommendations for both groups to be considered. In addition, however, both technology firms and the U.S. government will need to focus significant energy and resources (diplomatic and financial) to make the case against localization. As a general approach (as distinct from specific recommendations), both should work to correct pervasive misunderstandings about the benefits and drawbacks of data localization among policymakers, industry groups, civil liberty organizations, and other key stakeholders in nations considering such policies. They should forthrightly acknowledge the tremendous harm caused by the conduct of the NSA and by the companies that facilitated that conduct, and seek to rebuild, to the extent possible, global trust in the reliability of U.S. technology firms. In so doing, both are well advised to recognize the ambitions of the many interest groups advocating localization, and without compromising fundamental business or state interests, work to find a means to assist those groups in the realization of those ambitions.

A. *Recommendations for the U.S. Government*

1. Reform U.S. intelligence collection law and processes in line with the President's Review Group on Intelligence and Communications Technologies[126] and Privacy and Civil Liberties Oversight Board.[127]

The primary justification raised in favor of data localization policies is the need to protect citizens and companies from government surveillance of the like orchestrated by the NSA and other U.S. intelligence agencies. While the U.S. government should not compromise what it perceives as essential national security objectives in the face of threats to American business interests (especially in light of the hypocrisy involved in some of those threats), it should nevertheless seriously address the concerns of the international community about U.S. surveillance. Specifically, the U.S. can start by adopting some of the important recommendations of the President Review Group on Communications and Technologies, in particular, "Chapter IV: Reforming Foreign Intelligence Surveillance Directed at Non-United States Person," recommendations 12-15, focusing on reforming section 702 of the Foreign Intelligence Surveillance Act, such as applying the 1974 Privacy Act to non-U.S. persons. In addition, the U.S. also should consider recommendations of the Privacy and Civil Liberties Oversight Board for reforming section 702-based collections, importantly Recommendation #1 (a), "specify criteria for

---

in ten respondents report that they are changing their cloud purchasing decisions as a result of the Snowden disclosures. http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

[126] The President Review Group, Ibid.

[127] For more information, see the website of the Privacy and Civil Liberties Oversight Board, established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, and signed into law in August 2007, available at http://www.pclob.gov/about-us

determining the expected foreign intelligence value of a particular target,"[128] in order to ensure that foreign surveillance is undertaken only when there is a substantive national security need. These are serious recommendations, and their implementation ought to go a long way towards reducing (though surely not eliminating) international concerns over the surveillance policies of the United States. Implementation will demonstrate a willingness on the part of the U.S. government to respect global opinion and to impose limits on the reach of its intelligence agencies.

2. Create (or refocus) a senior U.S. government position to serve as the primary contact person and advocate for U.S. industry global data issues.

At present, there is no single point-person in the U.S. government coordinating data flow issues, or advocating on behalf of the U.S. for freedom of data flows. The head of the Federal Trade Commission, the U.S. Trade Representative, the Privacy and Civil Liberties Oversight Board, the Department of Commerce (importantly, the Deputy Assistant Secretary for Services), the Chief Privacy Officer of the NSA, several individuals within the Department of State (importantly the U.S. Coordinator for International Communications and Information Policy) as well as many, many others, are all working on the problem, but largely separately, with inevitably separate institutional viewpoints and objectives.

While multiple individuals and agencies should be addressing the issue simultaneously, there is a need for a single coordinating office to track and manage this vital economic issue. Perhaps an office of Chief Privacy Officer in the U.S. State Department and/or U.S. Trade Representative could be developed, or the newly created White House Chief Privacy Officer position could take on this broader international responsibility. President Obama has suggested, in a speech delivered at the U.S. Department of Justice on January 17, 2014, that his administration plans to create a new position at the U.S. State Department "to coordinate [American] diplomacy on issues related to technology and signals intelligence."[129] This new role—which has only been vaguely described —could also potentially fill the leadership vacuum within the U.S. government on these issues. However the reorganization happens, is clear that the current bureaucratic arrangement needs to be restructured to ensure that the anti-localization outreach strategy is effectively coordinated and

---

[128] Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 2 July 2014, available at http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf.

[129] "Remarks by the President on Review of Signals Intelligence," 17 January 2014, available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

harmonized across the entire U.S. government and among U.S. industry leaders.

3. Reform and streamline the Mutual Legal Assistance Treaty process.

The cumbersome MLAT process has proven to be one of the leading motivations behind many localization proposals. In order to expedite the MLAT process, the Department of Justice's should develop an online MLAT submission form, and devote the resources necessary to respond in a timely fashion, recognizing the urgency of many law enforcement requirements. In addition, the Department of Justice should (consistent with the reasonable confidentiality requirements of sound law enforcement) also publish regular government transparency reports, including breakdowns of number of requests received from different countries, the response provided, the crimes to which the requests relate, and the time each request required, and should provide clear, public guidance on what information can be obtained through an MLAT. These reports would not only result in an anticipated speed-up of response time (no one wants publicly to be shown to be dilatory), but would also demonstrate to foreign law enforcement personnel that their queries are receiving treatment not meaningfully less prompt than are other nations' requests of a similar nature.[130]

4. Consider adding Germany (and perhaps France and other European nations) to the "Five Eyes" intelligence sharing group, or another intelligence-sharing organization and agreement.

This recommendation may be the most difficult for the United States government to entertain, because, as we know, intelligence agencies are loathe to share their information, even with sister agencies within their own governments. Nevertheless, the United States surely recognizes that Germany, France, and other European nations have become essential partners in a variety U.S. national security endeavors over the past decade, assisting in national security operations from Afghanistan to Libya, and perhaps most significantly, in anti-terrorism. Yet these nations, and especially Germany (and to a lesser degree, France) have been especially troubled by the Snowden disclosures, in

[130] The Commerce, Justice, and Science Subcommittee appropriations bill of May 2014 provided the Department of Justice's criminal division with a $21 million increase over FY14, according to the department's budget request. The increase is (at least partly) designed to help DOJ streamline its ability to handle foreign data requests, a fix that tech companies have been clamoring for. "The Committee understands this funding will support additional positions and one-time costs associated with upgrading the case management system for MLAT processing," the report released by the committee states. This is an important first step, but money is only part of the solution. See Alex Byers, "Plus: Funding Bill Gives DOJ Cash for MLAT Reform," *Politico*, 9 May 2014, available at http://www.politico.com/morningtech/0514/morningtech13889.html.

large part due to the fact that the U.S. is supposed to be an ally. As Viviane Reding, a European Commission Vice President, lamented (surely disingenuously), "Friends and partners do not spy on each other."[131] In response, some U.S. lawmakers have proposed the idea of including Germany in the privileged "five eyes" intelligence group,[132] the group of the U.S., U.K., Australia, Canada, and New Zealand that generally agree not to monitor each other's officials or to conduct spying operations on each other's soil. It is a proposal that merits continued discussion, as would the inclusion of France, the Scandinavian nations, Holland, and perhaps others.[133] To the extent that these friendly governments are recipients of significant American intelligence information, they are likely to accept as credible future American assurances that their citizens, their leadership and their companies are not the subject of broad surveillance (or, if they are so subject, the sound security reasons for that surveillance).

5. Elevate the issue of data flows within the global trade bodies; include data flow issues within existing and future trade negotiations.

To the extent possible, the U.S. government should elevate data localization and global data flow issues within the global trade bodies, including the G8, G20, APEC, OECD, and WTO. Towards that end, the U.S. should strongly identify data restrictions as a global barrier to economic growth and trade. In addition, the U.S. should use multilateral trade negotiations, such as the Trans Pacific Partnership, the Transatlantic Trade and Investment Partnership, and the Trade in Services Agreement, as well as bilateral trade negotiations, to include provisions on open data flows.[134]

B. *Recommendations for U.S. Industry*

6. Encourage independent studies on the potential economic and security impacts of data localization for the countries considering them, and disseminate the findings of those studies to key global stakeholders.

A March 2014 survey by NTT Communications of over 1000 "IT decision-makers" found that ICT decision-makers are broadly in favor of

---

[131] Tony Fromm and Erin Mershon, "EU to DC: Friends do not spy on each other," *Politico*, 29 October 2013, available at http://www.politico.com/story/2013/10/european-union-nsa-friends-do-not-spy-on-each-other-99035.html.

[132] Antje Passenheim, "US lawmakers push for German entrance to Five Eyes spy alliance," *Deutsche Welle*, 22 November 2013, available at http://www.dw.de/us-lawmakers-push-for-german-entrance-to-five-eyes-spy-alliance/a-17246049.

[133] These nations are already part of other intelligence-sharing agreements, such as the so-called "nine eyes" and "fourteen eyes," but perhaps greater formalized information sharing agreements should be considered.

[134] See Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, Ibid.

localization measures.[135] Part of the reason this may be the case is that too few leaders are aware of the potential negative effects of such policies. They should be exposed to analyses not tainted by national or industry self-interest. To that end, industry ought to encourage the production of truly disinterested, peer-reviewed studies of the economic, security, and other effects of localization, and the dissemination of these studies to key stakeholders around the globe.

7. Work to reframe the privacy and surveillance discussion to one of security and economics.

Localization has been debated since the beginning of Snowden's revelations largely as an answer to privacy and surveillance concerns. Certainly, there is another "narrative" worthy of discussion, and to that end industry should work to alter the one-sided nature of the current discussion by including the issues of cybersecurity, cyber crime, economic integration, and Internet freedom. For developed countries, messaging to counter localization should focus on the urgent need to combat cybercrime and improve cyber security,[136] the adverse effects on freedom of expression, and interference with the expansion of Internet-borne commerce at just the time that their economies are emerging from the Great Recession. These views might resonate within developing countries as well, as would the additional argument that localization could leave them permanently on the poorer side of the "digital divide."

8. To the extent commercially and logistically possible, encrypt all user traffic to reassure customers of the security of their data.

In order to reassure foreign customers (as well as American customers for that matter), U.S. technology companies should seek to encrypt all data traffic. Encrypting information flowing among servers will not make it impossible for intelligence agencies to snoop on individual users of Internet services, and it will not have any significant effect on valid subpoenas for data. Still,

---

[135] The study found that 82 percent of ICT decision-makers are agree with proposals by German Chancellor Angela Merkel for separating data networks, and 95 percent of respondents believe that data location matters when it comes to storing company data. "NSA After-shocks: How Snowden has changed ICT decision-makers approach to the cloud," NTTC Report, March 2014, available at http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

[136] For this reframing to be viewed as authentic by nations around the globe, the U.S. government ought to collaborate with the private sector to prioritize the security of the entire network over specific intelligence collection goals. For instance, when the U.S. government learns of major Internet security flaws, the government should disclose those vulnerabilities responsibly to the public. President Obama has made important overtures in that direction, but those overtures must be more than simply rhetoric. See David Sanger, "Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say," *The New York Times*, 12 April 2014, available at http://www.nytimes.com/2014/04/13/us/politics/after-heartbleed-bug-obama-decides-us-should-reveal-internet-security-flaws.html.

widespread use of encryption technology makes mass surveillance more difficult, whether conducted by governments or other sophisticated hackers, and would serve to give customers some reason to believe that American firms were sensitive to their concerns. Facebook and Yahoo have already begun encrypting traffic between their internal servers;[137] Google, likewise, has launched a campaign to boost encryption of its Gmail services and has released the source code for a browser extension allowing 'end-to-end' encryption of browsing data.[138] These are important efforts, but more could be done.

9. Expand joint ventures with foreign enterprises, and increase technology sharing, particularly with companies in developing countries.

The calls for localization may be muted if American technology firms can be seen as supportive of foreign enterprises, and particularly of the efforts of developing countries to build Internet sectors able to provide efficient and inexpensive services to their populations. To that end, American companies ought to use some of their resources to launch joint ventures with foreign companies, especially companies in the developing world. This process will inevitably entail some technology transfers with the attendant risk of the loss of proprietary intellectual property, but the mitigation of that risk is largely within the control of the sharing company, unlike the political risks involved in data localization. While joint ventures and technology sharing would be especially welcome in developing countries (and thus turn down the heat generated by their political elites), ventures with the companies of developed countries might also serve the anti-localization cause—would Deutsche Telekom be so eager to exclude American companies if it would profit more immediately, and perhaps more securely, as a partner, rather than as a competitor, of its American counterparts?

VII. CONCLUSION

In little more than two decades, the Internet has gone from a research tool and plaything of academics and engineers to a dominant force—perhaps *the* dominant force—in the world's culture, economy and politics. In its gestational years, governments did not pay much attention to it. For obvious reasons, governments are no longer indifferent, nor should they be. Where such massive power exists, there must be regulation to protect citizens from the misuse of that power. But writing regulations for the Internet requires a remarkably delicate hand, and data localization is anything but delicate. Indeed,

---

[137] David E. Sanger and Nicole Perlroth, 6 June 2014. Ibid.
[138] "Making end-to-end encryption easier to use," *Google Online Security Blog*, 3 June 2014, available at http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html

it is not unreasonably alarmist to suggest that localization policies present a serious threat to all parties who are beneficiaries of the Internet.