DATA NATIONALISM

Anupam Chander[*]
Uyên P. Lê[**]

ABSTRACT

A BRICS Internet, the Euro Cloud, the Iranian "Halal" Internet: Governments across the world eager to increase control over the World Wide Web are tearing it apart. Iran seeks to develop an Internet free of Western influences or domestic dissent. The Australian government places restrictions on health data leaving the country. Russia requires personal information to be stored domestically. Vietnam insists on a local copy of all Vietnamese data. The last century's nontariff barriers to goods have reappeared as firewalls blocking international services. Legitimate global anxieties over surveillance and security are justifying governmental measures that break apart the World Wide Web, without enhancing either privacy or security.

The issue is critical to the future of international trade and development, and even to the ongoing struggle between democracy and totalitarianism. Data localization threatens the possibility of outsourcing services, whether to Bangalore, Accra, Manila, or even Silicon Valley. The theory of this Article expands the conversation about international Internet regulation from efforts to prevent data from flowing in to a country through censorship, to include efforts to prevent data from flowing out through data localization. A simple formula helps demonstrate what is stake: censorship + data localization = total control.

---

[*] Director, California International Law Center, Professor of Law and Martin Luther King, Jr. Hall Research Scholar, University of California, Davis; A.B., Harvard College; J.D., Yale Law School. We are grateful for a Google Research Award, which helped support this work. We thank Katherine Linton and Michael Stanton-Geddes of the International Trade Commission for helpful conversations, and Varun Aery, Joey Deleon, Poomsiri Dumrongvute, Aigerim Dyussenova, Jordy Hur, Taejin Kim, Meimei Li, Pricillia Haesanny, Laura Pedersen, Rachael Smith, and Radhika Tahiliani for very helpful research and translation assistance. We are also grateful for the superb editing of the *Emory Law Journal* staff, especially Executive Managing Editor Ryan Rummage and Editor in Chief Benjamin Klebanoff. The views expressed herein are the authors' alone, as are any errors.

[**] Free Speech and Technology Fellow, California International Law Center; A.B., Yale College; J.D., University of California, Davis School of Law.

INTRODUCTION

The era of a global Internet may be passing. Governments across the world are putting up barriers to the free flow of information across borders. Driven by concerns over privacy, security, surveillance, and law enforcement, governments are erecting borders in cyberspace, breaking apart the World Wide Web. The first generation of Internet border controls sought to keep information out of a country—from Nazi paraphernalia to copyright infringing material.[1] The new generation of Internet border controls seeks not to keep information out but rather to keep data in. Where the first generation was relatively narrow in the information excluded, the new generation seeks to keep all data about individuals within a country.

Efforts to keep data within national borders have gained traction in the wake of revelations of widespread electronic spying by United States intelligence agencies.[2] Governments across the world, indignant at the recent disclosures, have cited foreign surveillance as an argument to prevent data from leaving their borders, allegedly into foreign hands.[3] As the argument

---

[1] *See* Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, D. 2000 inf. rap. 172, obs. J. Gomez, *available at* http://juriscom.net/2000/05/tgi-paris-refere-22-mai-2000-uejf-et-licra-c-yahoo-inc-et-yahoo-france/, *translation available at* http://www.lapres.net/yahen.html (Daniel Arthur Laprès, trans.); Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, JCP 2000, Actu., 2219, obs. J. Gomez (Fr.), *available at* http://juriscom.net/wp-content/documents/tgiparis20001120.pdf, *translation available at* http://www.lapres.net/yahen11.html (Daniel Arthur Laprès, trans.); *see also* Yahoo! Inc. v. La Ligue Cotnre le Racisme et L'Antisemtisime, 433 F.3d 1199 (9th Cir. 2006) (en banc) (per curiam) (discussing the French proceedings and parallel proceedings in the United States). For a domestic example, see Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011), which was ostensibly designed to require internet service providers to block access to foreign websites hosting copyright infringing materials.

[2] The disclosures based on Edward Snowden's documents began with the following article: Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 06.05 EDT), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Earlier accounts of the NSA's global surveillance plans include James Bamford, *The Black Box*, WIRED, Apr. 2012, at 78, *available at* http://www.wired.co.uk/magazine/archive/2012/05/features/the-black-box. Such intelligence gathering is hardly limited to the United States, of course. David E. Sanger, David Barboza & Nicole Perlroth, *China's Army Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 19, 2013, at A1, *available at* http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html (describing hacking of United States computer networks, apparently from China); *see also* Ewen MacAskill et al., *GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications*, GUARDIAN (June 21, 2013, 12:23 EDT), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (describing United Kingdom surveillance of global communications).

[3] *See* Bundesregierung, *Merkel: Neue Projekte mit Frankreich* [*Merkel: New Projects with France*], YOUTUBE (Feb. 15, 2014), https://www.youtube.com/watch?v=MQo1mcyDvUg (showing German Chancellor Angela Merkel's discussion of European data protection); Max Smolaks, *Russian Government Will Force Companies to Store Citizen Data Locally*, TECHWEEK EUR. (July 4, 2014, 17:22), http://www.techweekeurope.co.uk/news/russian-government-will-force-companies-store-citizen-data-locally-148560 (noting that Russia's

goes, placing data in other nations jeopardizes the security and privacy of such information. We define "data localization" measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of forms—including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data. We argue here that data localization will backfire and that it in fact undermines privacy and security, while still leaving data vulnerable to foreign surveillance. Even more importantly, data localization increases the ability of governments to *surveil* and even oppress their own populations.

Imagine an Internet where data must stop at national borders, examined to see whether it is allowed to leave the country and possibly taxed when it does. While this may sound fanciful, this is precisely the impact of various measures undertaken or planned by many nations to curtail the flow of data outside their borders. Countries around the world are in the process of creating Checkpoint Charlies—not just for highly secret national security data but for ordinary data about citizens. The very nature of the World Wide Web is at stake. We will show how countries across the world have implemented or have planned dramatic steps to curtail the flow of information outside their borders. By creating national barriers to data, data localization measures break up the World Wide Web, which was designed to share information across the globe.[4] The Internet is a global network based on a protocol for interconnecting computers without regard for national borders. Information is routed across this network through decisions made autonomously and automatically at local routers, which choose paths based largely on efficiency, unaware of political borders.[5] Thus, the services built on the Internet, from email to the World

"legal measure is widely seen as a response to reports about the intrusive surveillance practices of the US National Security Agency (NSA) and the UK's GCHQ"); Thomas K. Thomas, *Route Domestic Net Traffic via India Servers, NSA Tells Operators*, HINDU BUS. LINE (Aug. 14, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece (stating that India's Deputy National Security Advisor has reportedly sought "ways to route domestic Internet traffic via servers within the country," and quoting an official who said that "[s]uch an arrangement would limit the capacity of foreign elements to scrutinise intra-India traffic").

[4] *See* TIM BERNERS-LEE WITH MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 4 (1999) (describing a vision of a "single, global information space").

[5] For a brief overview of the architecture of the Internet, see ETHAN ZUCKERMAN & ANDREW MCLAUGHLIN, INTRODUCTION TO INTERNET ARCHITECTURE AND INSTITUTIONS (2003), *available at* http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.pdf.

Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making the physical locations for the storage and processing of their data largely invisible to users. Data localization would dramatically alter this fundamental architecture of the Internet.

Such a change poses a mortal threat to the new kind of international trade made possible by the Internet—information services such as those supplied by Bangalore or Silicon Valley.[6] Barriers of distance or immigration restrictions had long kept such services confined within national borders. But the new services of the Electronic Silk Road often depend on processing information about the user, information that crosses borders from the user's country to the service provider's country. Data localization would thus require the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs and other burdens enormously for both providers and consumers and rendering many of such global services impossible.

While others have observed some of the hazards of data localization, especially for American companies,[7] this Article offers three major advances over earlier work in the area. First, while the earlier analyses have referred to a data localization measure in a country in the most general of terms, our Article provides a detailed legal description of localization measures. Second, by examining a variety of key countries around the world, the study allows us to see the forms in which data localization is emerging and the justifications offered for such measures in both liberal and illiberal states. Third, the Article works to comprehensively refute the various arguments for data localization offered around the world, showing that data localization measures are in fact likely to undermine security, privacy, economic development, and innovation where adopted.

---

[6] *See* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD 2–3 (2013).

[7] *See, e.g.*, BUS. ROUNDTABLE, PROMOTING ECONOMIC GROWTH THROUGH SMART GLOBAL INFORMATION TECHNOLOGY POLICY: THE GROWING THREAT OF LOCAL DATA SERVER REQUIREMENTS (2012), *available at* http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf; DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? (2013), *available at* http://www2.itif.org/2013-cloud-computing-costs.pdf; STEPHEN J. EZELL, ROBERT D. ATKINSON & MICHELLE A. WEIN, INFO. TECH. & INNOVATION FOUND., LOCALIZATION BARRIERS TO TRADE: THREAT TO THE GLOBAL INNOVATION ECONOMY (2013), *available at* http://www2.itif.org/2013-localization-barriers-to-trade.pdf; EDWARD GRESSER, PROGRESSIVE ECON., 21ST-CENTURY TRADE POLICY: THE INTERNET AND THE NEXT GENERATION'S GLOBAL ECONOMY (2014), *available at* http://progressive-economy.org/files/2014/01/21st.Century.Trade_.pdf; U.S. INT'L TRADE COMM'N, PUB. 4415, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 1 (2013), *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

Our paper proceeds as follows. Part I describes the particular data localization measures in place or proposed in different countries around the world, as well as in the European Union. Part II then discusses the justifications commonly offered for these measures—such as avoiding foreign surveillance, enhancing security and privacy, promoting economic development, and facilitating domestic law enforcement. We appraise these arguments, concluding that, in fact, such measures are likely to backfire on all fronts. Data localization will erode privacy and security without rendering information free of foreign surveillance, while at the same time increasing the risks of domestic surveillance.

I. COUNTRY STUDIES

We review here data localization measures in seventeen states—Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Kazakhstan, Malaysia, Nigeria, Russia, South Korea, Sweden, Taiwan, Thailand, and Vietnam—as well as the European Union and a handful of other countries in less detail. The problem of data localization is even more pervasive than the jurisdictions we identify. Furthermore, the measures achieve data localization in a wide variety of ways. While some of the measures explicitly force data to be located on home country servers, often the localizing effect is less visible and more indirect. Kazakhstan's directive, for example, is explicit, requiring new companies using the ".kz" top level domain to operate from physical servers located within the country.[8] Malaysia, on the other hand, requires consent for international transfer of data, which can prove a significant hurdle.[9] Taiwan permits authorities to restrict transfers if they concern "major national interests."[10] Other regulations focus on selected sectors. Australia prevents health records from being transferred outside the country if they are personally identifiable.[11] In sum, our study reveals the astonishing array of countries that have enacted or are considering data localization.

---

[8] FREEDOM HOUSE, FREEDOM ON THE NET 2013: A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA 441 (Sanja Kelly et al. eds., 2013), *available at* http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.

[9] Personal Data Protection Act 2010 § 129 (Act No. 709) (Malay.), *available at* http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.

[10] Personal Information Protection Act (promulgated by the Ministry of Justice, May 26, 2010), art. 21 (Taiwan), *available at* http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021.

[11] *Personally Controlled Electronic Health Records Act 2012* (Cth) s 77 (Austl.).

A. Australia

In 2012, Australia passed the Personally Controlled Electronic Health Records (PCEHR) Act, Section 77 of which prohibits the transfer of health records outside of Australia, with certain exceptions.[12] Subsection 1 provides:

> The System Operator, a registered repository operator, a registered portal operator or a registered contracted service provider that holds records for the purposes of the PCEHR system (whether or not the records are also held for other purposes) or has access to information relating to such records, must not: (a) hold the records, or take the records, outside Australia; or (b) process or handle the information relating to the records outside Australia; or (c) cause or permit another person: (i) to hold the records, or take the records, outside Australia; or (ii) to process or handle the information relating to the records outside Australia.[13]

Subsection 2 permits the transfer, processing, or handling of data outside of Australia if such records do not include "personal information in relation to a consumer" or "identifying information of an individual or entity."[14]

In essence, under these provisions, foreign companies handling health-related information must build data centers or outsource to local services inside Australia. It also raises practical issues for users who wish to access their data from overseas.[15]

B. Brazil

In 2011, Brazil's Congress began considering the *Marco Civil da Internet*, a landmark bill that would guarantee Brazilians a significant array of civil

---

[12] *Id.*

[13] *Id.* s 77(1).

[14] *Id.* s 77(2).

[15] An Australian local healthcare provider worried that the law would be difficult to operationalize in a world where Australians carried mobile devices as they traveled overseas. CSC, CSC'S SUBMISSION TO THE STANDING COMMITTEE ON COMMUNITY AFFAIRS: INQUIRY INTO THE PROVISIONS OF THE PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORDS BILL 2011 AND A RELATED BILL 7 (2011), *available at* https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=f9019a89-8166-42a4-b733-3b7d87f4afc3. The provider observed, "Consumers will access their data via mobile devices overseas and this will result in data, de facto, being accessed and potentially held or cached, outside of Australia." *Id.*; *see also* Josh Taylor, *E-health Law to Block Overseas Access: CSC*, ZDNET (Jan. 9, 2012, 06:04 GMT), http://www.zdnet.com/e-health-law-to-block-overseas-access-csc-1339329216/ (examining CSC's submission to parliament).

rights online.[16] Some in the Internet community described it as an "anti-ACTA," referring to the proposed Anti-Counterfeiting Trade Agreement that would have enhanced government and private powers on behalf of intellectual property holders.[17] Others described the bill as a "ground-breaking internet bill of rights."[18]

After the NSA surveillance revealed that the U.S. had surveilled both President Dilma Rousseff and Brazil's largest company, Petrobras,[19] a new version of the bill was introduced by House of Representatives Framework Rapporteur Alessandro Molon (Workers Party Member from Rio de Janeiro) at the request of President Rousseff.[20] This version included a new power for the executive branch: the ability to require that data about Brazilians be stored in Brazil.[21] Article 12 of the new proposed *Marco Civil* provided as follows:

> The Executive branch, through Decree, may force connection providers and Internet applications providers provided for in art. 11, who exercise their activities in an organized, professional and economic way, to install or use structures for storage, management

---

[16] *See* Letter from Dean C. Garfield, President & CEO, Info. Tech. Indus. Council, to the Honorable Gleisi Helena Hoffmann, Minister, Casa Civil, Presidency of the Republic (Aug. 5, 2013), *available at* http://www.itic.org/dotAsset/2a6d7008-9c61-4f7c-917a-5fe4ad493527.pdf. The *Marco Civil* was inspired by the work of Ronaldo Lemos. *See* Ronaldo Lemos, *Internet brasileira precisa de marco regulatório civil* [*Brazilian Internet Needs Civil Regulatory Framework*], UOL (May 22, 2007, 21h13), http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm (Braz.).

[17] *See* Glyn Moody, *Brazil Drafts an 'Anti-ACTA': A Civil Rights-Based Framework for the Internet*, TECHDIRT (Oct. 4, 2011, 1:12 PM), http://www.techdirt.com/articles/20111004/04402516196/brazil-drafts-anti-acta-civil-rights-based-framework-internet.shtml.

[18] *Everything is Connected*, ECONOMIST, Jan. 5, 2013, at 17, *available at* http://www.economist.com/news/briefing/21569041-can-internet-activism-turn-real-political-movement-everything-connected.

[19] *See* Glenn Greenwald, Robert Kaz & José Casado, *EUA Espionaram Milhões de E-mails e Ligações de Brasileiros* [*US Spied on Millions of Emails and Calls from Brazil*], O GLOBO MUNDO (Dec. 7, 2013, 19:50), http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2lEHZqYwh (Braz.); Angelica Mari, *Brazilian Government Tries to Deal with NSA Spying*, ZDNET (July 8, 2013, 17:06 GMT), http://www.zdnet.com/brazilian-government-tries-to-deal-with-nsa-spying-7000017771/; Jonathan Watts, *NSA Accused of Spying on Brazilian Oil Company Petrobras*, GUARDIAN (Sept. 9, 2013, 11:55 EDT), http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras; Brian Winter, *Exclusive: Brazil's Rousseff Wants U.S. Apology for NSA Spying*, REUTERS, Sept. 4, 2013, *available at* http://www.reuters.com/article/2013/09/04/us-usa-security-snowden-brazil-idUSBRE98314N20130904.

[20] *Brazilian President Pursues Server Localization Policies*, WHITE & CASE LLP (Jan. 2014), http://www.whitecase.com/alerts-01082014-2/#.VFU9lPTF9pY; *see also* Dilma Rousseff, President of the Federative Republic of Brazil, Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly (Sept. 24, 2013), *available at* http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf [hereinafter Statement by Dilma Rousseff].

[21] Substitutivo ao Projeto de Lei n. 2126 de 2011 [Substitutive Bill Proposal to Draft Law No. 2126 of 2011], *translation available at* http://www.ip-watch.org/weblog/wp-content/uploads/2013/11/MC_Eng_CR_Nov_13_2013.docx (Carolina Rossini, trans.).

> and dissemination of data in the country, considering the size of the providers, its sales in Brazil and breadth of the service offering to the Brazilian public.[22]

Internet companies found in violation could face a "fine of up to ten percent of the [previous year's] gross revenues" from their activities in Brazil.[23] After consideration, however, the *Marco Civil* was passed into law on April 23, 2014, without the much-debated data localization provision.[24]

C. Canada

While Canada's national law, the Personal Information Protection and Electronic Documents Act (PIPEDA),[25] does not prohibit the transfer of personal data outside of Canada, cross-border data flow faces provincial prohibitions. These provincial restraints developed out of attempts to outsource government information technology services to providers based in the United States.[26] While these rules were formulated long before the Snowden revelations, they were justified by increases in the U.S. government's surveillance power provided in the USA PATRIOT Act.[27]

Two Canadian provinces, British Columbia and Nova Scotia, have enacted laws requiring that personal information held by public institutions—schools, universities, hospitals, government-owned utilities, and public agencies—be stored and accessed only in Canada unless one of a few limited exceptions applies.[28]

British Columbia's 1996 Freedom of Information and Protection of Privacy Act states, "A public body must ensure that personal information in its custody

---

[22] *Id.* art. 12.

[23] *Id.* art. 13.

[24] *See* Philippe Bradley & Dan Cooper, *Brazil Enacts "Marco Civil" Internet Civil Rights Bill*, INSIDEPRIVACY (Apr. 28, 2014), http://www.insideprivacy.com/international/brazil-enacts-marco-civil-internet-civil-rights-bill/ (blog maintained by Covington & Burling discussing the Marco Civil law).

[25] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Can.).

[26] *See* FRED H. CATE, CTR. FOR INFO. POLICY LEADERSHIP, PROVINCIAL CANADIAN GEOGRAPHIC RESTRICTIONS ON PERSONAL DATA IN THE PUBLIC SECTOR 3–4 (2008), *available at* http://www.hunton.com/files/Publication/2a6f5831-07b6-4300-af8d-ae30386993c1/Presentation/PublicationAttachment/0480e5b9-9309-4049-9f25-4742cc9f6dce/cate_patriotact_white_paper.pdf.

[27] *See id.*

[28] *See* Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1 (Can.), *available at* http://www.bclaws.ca/Recon/document/ID/freeside/96165_00; Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1) (Can.), *available at* http://www.canlii.org/en/ns/laws/stat/sns-2006-c-3/latest/sns-2006-c-3.html.

or under its control is stored only in Canada and accessed only in Canada."[29] Exceptions to this requirement include situations in which the data subject "has identified the information and has consented . . . to it being stored in or accessed from . . . another jurisdiction."[30] Nova Scotia provides a similar localization mandate,[31] but its law also permits storage or access outside of Canada if the "head of a public body" determines that it is necessary for the public body's operation.[32]

Consider the implications of British Columbia's rule for the use of a foreign email service. If an individual uses Google's Gmail (presumably based in the United States), not only would she have to consent to the transfer of information to the United States, but every Canadian she talks about in her Gmail email messages would have to consent as well.[33]

D. China

Localization obligations exist in certain Chinese sector-specific operations. In 2011, the People's Bank of China (PBOC) issued a Notice to Urge Banking Financial Institutions to Protect Personal Financial Information.[34] Chinese banks and foreign invested commercial banking institutions "are required to observe [this Notice] when collecting, processing and storing personal financial information (PFI)."[35] The Notice "prohibits Banks from storing, processing or analysing outside China any PFI which has been collected in China, or providing PFI collected in China to an offshore entity."[36] Banks outsourcing their data outside of China need to pay special attention to this requirement, especially as the Notice defines PFI very broadly, including

---

[29] Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, at c. 165, s. 30.1.

[30] *Id.* s. 30.1(a).

[31] Personal Information International Disclosure Protection Act, S.N.S. 2006, at c. 3, s. 5(1)(a)–(b).

[32] *Id.* s. 5(2).

[33] *See* CHANDER, *supra* note 6, at 6.

[34] Zhongguorenmin Yinhang Guanyu Yinhangye Jinrong Jigou Zuo Hao Geren Jinrong Xinxi Baohu Gongzuo de Tongzhi (中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知) [Notice on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information] (promulgated by the People's Bank of China, Jan. 21, 2011) (Lawinfochina) (China), *available at* http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid=; Gigi Cheah, *Protection of Personal Financial Information in China*, NORTON ROSE FULBRIGHT (Oct. 10, 2011), http://www.nortonrosefulbright.com/knowledge/publications/56148/protection-of-personal-financial-information-in-china.

[35] *See* Cheah, *supra* note 34.

[36] *See id.*

personal information of identity, property, account, credit, financial transaction, etc.[37]

In 2013, the Chinese government issued the Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (the Guidelines).[38] Although the Guidelines are a voluntary technical guidance document,[39] they might serve as a regulatory baseline for Chinese judicial authorities and lawmakers.[40] The Guidelines prohibit the transfer of personal data abroad without express consent of the data subject or explicit regulatory approval. Article 5.4.5 of the Guidelines provides as follows:

---

[37] *See id.* The United States Federal Reserve has simply asked banks to examine the risks associated with outsourcing, whether within the United States or offshore. BD. OF GOVERNORS OF THE FED. RESERVE SYS., GUIDANCE ON MANAGING OUTSOURCING RISK (2013), *available at* http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf.

[38] On July 16, 2013, China's Ministry of Industry and Information Technology (MIIT) promulgated the Provisions on Protecting the Personal Information of Telecommunication and Internet Users (the Provisions), which went into effect on September 1, 2013. Dianxin He Hulianwangyonghu Geren Xinxi Baohu Guiding (电信和互联网用户个人信息保护规定) [Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Indus. & Info. Tech. July 16, 2013, effective, Sept. 1, 2013) (Lawinfochina) (China), *available at* http://www.lawinfochina.com/display.aspx?id=14971&lib=law&SearchKeyword=personal%20information&SearchCKeyword=. The Provisions provide implementing rules for the Decision on Strengthening Protection of Online Information (the Decision), a national law issued in December 2012. *See China Dives into Data Protection Regulation*, TAYLORWESSING (Apr. 2013), http://www.taylorwessing.com/globaldatahub/article_china_dp.html ("The [National People's Congress] rolled out its *Decision on Strengthening Internet Information Protection* (Decision) on 28 December 2012."); *see also MIIT Issues Comprehensive Regulation on Collection and Use of Personal Information by Internet and Telecommunication Service Providers*, LEHMAN, LEE & XU, http://www.lehmanlaw.com/resource-centre/faqs/information-technology/miit-issues-comprehensive-regulation-on-collection-and-use-of-personal-information-by-internet-and-telecommunication-service-providers.html (last visited Feb. 6, 2015). These provisions are in addition to the Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems, promulgated on January 21, 2013, which became effective February 1, 2013. A translation of these Guidelines composed by Dr. George Yijun Tian, in addition to an overview of them, can be found in Graham Greenleaf & George Yijun Tian, *China Expands Data Protection through 2013 Guidelines*, PRIVACY L. & BUS. INT'L REP., Apr. 2013, at 1 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280037 [hereinafter Guidelines].

[39] Daniel Cooper, Eric Carlson & Scott Livingston, *China Releases New National Standard for Personal Information Collected over Information Systems*, COVINGTON & BURLING LLP (Feb. 15, 2013), http://www.cov.com/files/Publication/a180859b-c1ab-4ecf-a274-e6d1a7b5fb2e/Presentation/PublicationAttachment/c8aad899-85f3-4d26-bb06-f0518ee09e20/China_Releases%20_New_National_Standard_for_Personal_Information_Collected_Over_Information_Systems.pdf.

[40] Gao Chiyang, Deputy Director of China Software Testing Center, who drafted the Guidelines, noted that even though the Guidelines are voluntary, they can provide principles for upcoming legislations. *See* Zhao Zie (赵杰), *Geren Xinxi Baohu Lifa Shang wu Shijianbiao Qiye Cheng Xiemi Zhu Qyudao* (个人信息保护立法尚无时间表 企业成泄密主渠道) [*Personal Information Protection Legislation: There is No Timetable in the Main Channel of Business*], CHINA SEC. J. (Apr. 20, 2012, 13:57), http://www.cs.com.cn/xwzx/sz/201204/t20120420_3325052.html.

> Absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities, the administrator of personal information must not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas.[41]

The Law of the People's Republic of China on Guarding State Secrets prevents data from being removed from China if it is deemed to contain a state secret.[42] "State secrets" are "matters that have a vital bearing on state security and national interests,"[43] and include "secrets in national economic and social development," "secrets concerning science and technology," and even "[s]ecrets of political parties."[44]

E. European Union

The European Union's 1995 Data Protection Directive recognized that the free flow of data across borders was necessary to commerce.[45] At the same time, it sought to ensure that data about Europeans was well protected as it traveled the world.[46] Accordingly, it allowed data to be sent outside the European Union (or the European Free Trade Association states) if it were protected adequately either by local law or by contractual arrangement with the foreign company.[47] To date, the European Commission has found eleven

---

[41] Guidelines, *supra* note 38, at art 5.4.5.

[42] *See* Tom Antisdel & Tarek Ghalayini, *The Challenge of Conducting Data Collections and Investigations Under Unclear Data Privacy Rules*, CHINA BUS. REV., Oct.–Dec. 2011, at 46, 48, *available at* http://www.chinabusinessreview.com/the-challenge-of-conducting-data-collections-and-investigations-under-unclear-data-privacy-rules/.

[43] Zhonghua Renmin Gongheguo Baoshou Guojia Mimi Fa (中华人民共和国保守国家秘密法) [Law of the People's Republic of China on Guarding State Secrets] (promulgated by the Standing Comm. of the Nat'l People's Cong., Sept. 5, 1988, effective May 1, 1989), art. 2 (Lawinfochina) (China), *available at* http://www.lawinfochina.com/display.aspx?lib=law&id=1191&CGid=.

[44] *Id.* art. 8.

[45] *See* Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 36–37 [hereinafter Council Directive] ("Whereas cross-border flows of personal data are necessary to the expansion of international trade . . . .").

[46] *See id.* at 31 (showing that the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services, and capital is ensured requires not only that personal data should be able to flow freely from one Member State to another but also that the fundamental rights of individuals should be safeguarded).

[47] *See id.* at 37, 45–46. The Data Protection Directive typically limits the transfer of data outside the European Union or the European Free Trade Association unless the country to which it is exported has been adjudged by the European Commission as providing "an adequate level of protection" for data or where the foreign processor agrees to contractual protections for the data. *See id.*

jurisdictions as having adequate protection: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.[48] Given the amount of information exchanged with the United States, the European Union negotiated a special Safe Harbor with the United States, allowing data to be exported to companies in the United States that abide by certain data protection standards, under the supervision of the Federal Trade Commission.[49] Recently, however, the European Union has been reconsidering the Safe Harbor, alongside a major effort to rewrite European Union privacy law altogether.[50] The EU parliamentarian in charge of steering the European Commission's proposed data protection reform, Jan-Philipp Albrecht, released a report in 2013 recommending that the EU discontinue the Safe Harbor framework after enacting major privacy reforms.[51] After the NSA revelations broke, Vice President Viviane Reding declared that the Safe Harbor agreement "may not be so safe after all."[52] The European Parliament also requested the European Commission to review the Safe Harbor.[53] On November 27, 2013, the Commission published a set of recommendations that it asked the United States Department of Commerce to consider, with the possibility left open that the Safe Harbor might be suspended.[54]

---

[48] *See Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated Feb. 6, 2015).

[49] For the Safe Harbor Privacy Principles themselves, see Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666 (Dep't of Commerce July 24, 2000) (notice).

[50] Stephen Gardner, *Lead EU Lawmaker Report Seeks Changes to Proposed Data Protection Regulation*, BLOOMBERG BNA (Jan. 14, 2013), http://www.bna.com/lead-eu-lawmaker-n17179871844/.

[51] *See Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 198, COM (2012) 11 (Nov. 21, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//EN&language=en.

[52] *See* Christopher Wolf, *EU VP Reding Uses PRISM as Lever to Push Enactment of Regulation and Questions EU-US Safe Harbor*, CHRON. DATA PROTECTION (July 19, 2013), http://www.hldataprotection.com/2013/07/articles/international-eu-privacy/eu-vp-reding-uses-prism-as-lever-to-push-enactment-of-regulation-and-questions-eu-us-safe-harbor/.

[53] *See* Resolution on the US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy, EUR. PARL. DOC. RSP 2682 (2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN.

[54] *See Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final (Nov. 11, 2013) [hereinafter *Rebuilding Trust in EU-US Data Flows*], *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf; Stephen Gardner, *U.S. Officials Respond to EU Concerns Over Safe Harbor Data Transfer Program*, BLOOMBERG BNA (Dec. 16, 2013), http://www.bna.com/us-officials-respond-n17179880742/.

In October 2013, the European Parliament's Civil Liberties, Justice and Home Affairs Committee voted to advance a sweeping reform of EU data protection law titled the General Data Protection Regulation (the GDPR).[55] The GDPR allows companies to transfer data outside the European Union if appropriate safeguards are in place, such as binding corporate rules, a valid "European Data Protection Seal" for both controller and recipient, standard data protection clauses, or contractual clauses with prior authorization from the member state's data protection authority.[56] The draft would prohibit the transfer to a country where the law permits local authorities access to personal data from the European Union.[57] Currently, the draft is undergoing Parliament–Council negotiations, which were projected to conclude at the end of 2014.[58]

F. France

Citing both concerns about foreign surveillance and competitiveness, the French government has sought over the last few years to promote a local data center infrastructure, which some have dubbed "*le cloud souverain*," or the sovereign cloud.[59] The government has directly invested in two cloud computing enterprises, Numergy and Cloudwatt, with a one-third ownership stake in each.[60] In February 2013, Minister of Industry Arnaud Montebourg declared his support for efforts to keep data processing in France in order to support domestic employment.[61] Whether a subsidy to domestic enterprises is a

---

[55] Press Release, Comm. on Civil Liberties, Justice & Home Affairs, Eur. Parliament, Civil Liberties MEPs Pave the Way for Stronger Data Protection in the EU (Oct. 21, 2013), *available at* http://www.europarl.europa.eu/pdfs/news/expert/infopress/20131021IPR22706/20131021IPR22706_en.pdf.

[56] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Compromise Amendments on Articles 30–91*, at art. 42(1)–(4), COM (2012) 11 (Oct. 17, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

[57] *Id.* art. 41, recital 82.

[58] *Q&A on EU Data Protection Reform*, EUR. PARLIAMENT (Apr. 3, 2014, 09:04), http://www.europarl.europa.eu/pdfs/news/expert/background/20130502BKG07917/20130502BKG07917_en.pdf.

[59] *See* Jérôme Colombain, *La France Veut Son "Cloud Souverain"* [*France Wants His "Sovereign Cloud"*], FRANCE INFO (Apr. 16, 2012), http://www.franceinfo.fr/high-tech/nouveau-monde/la-france-veut-son-cloud-souverain-586813-2012-04-16.

[60] *See* David Meyer, *A Guide to the French National Cloud(s)*, GIGAOM (Nov. 18, 2013, 7:55 AM PST), http://gigaom.com/2013/11/18/a-guide-to-the-french-national-clouds/.

[61] *Arnaud Montebourg: «Google et Facebook agissent ainsi car il n'y a pas de règles»* [*Arnaud Montebourg: Google and Facebook are Doing this Because There are No Rules*], 20 MINUTES.FR (Feb. 28, 2013 09:29), http://www.20minutes.fr/politique/1109303-arnaud-montebourg-nous-faisons-tous-jours-lois-citoyens-pourquoi-contre-geants-linternet.

violation of trade commitments is a complicated question. The Snowden revelations spurred an additional push by the government to localize data in France: if the PRISM claim "turns out to be true, it makes [it] relatively relevant to locate datacentres and servers in [French] national territory in order to better ensure data security," the Digital Economy Minister Fleur Pellerin explained.[62] The government's ambition to promote a "Made in France" label includes efforts in cloud computing, big data, and connected devices.[63] In its national innovation plan, the government declared its goal to "build a France of digital sovereignty."[64]

Proposals to tax the "collection, management and commercial exploitation of personal data generated by users located in France" may well be implemented in a form designed to discourage services located outside the country.[65] Proponents of the tax, in fact, reveal that one goal of the tax is to "[p]romot[e] productivity gains and value creation in the domestic economy."[66] The so-called "data tax" would apply to "data derived from the *regular and systematic monitoring of users' activity*."[67] Under the proposal, the tax rate would depend on the level of compliance with respect to privacy, potentially diminishing to zero for those that were fully compliant.[68] If France were to declare that data processing in the United States was noncompliant, even when conducted under the Safe Harbor, such a tax would effectively

---

[62] *See* Valéry Marchive, *France Hopes to Turn PRISM Worries into Cloud Opportunities*, ZDNET (June 21, 2013, 9:02 GMT), http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/ (second alteration in original).

[63] *See* MINISTÈRE DU REDRESSEMENT PRODUCTIF [MINISTRY OF ECON. REGENERATION], THE NEW FACE OF INDUSTRY IN FRANCE 51, 53, 61 (2013), *available at* http://www.entreprises.gouv.fr/files/files/directions_services/secteurs-professionnels/industrie/nfi/NFI-anglais.pdf [hereinafter NEW FACE OF INDUSTRY]. President François Hollande announced a national innovation program on September 12, 2013. Nicholas Vinocur, *Hollande Turns to Robots, Driverless Cars to Revive French Industry*, REUTERS, Sept. 12, 2013, *available at* http://www.reuters.com/article/2013/09/12/us-france-industry-idUSBRE98B0HW20130912.

[64] NEW FACE OF INDUSTRY, *supra* note 63, at 51.

[65] PIERRE COLLIN & NICHOLAS COLIN, TASK FORCE ON TAXATION OF THE DIGITAL ECON., REPORT TO THE MINISTER FOR THE ECONOMY AND FINANCE, THE MINISTER FOR INDUSTRIAL RECOVERY, THE MINISTER DELEGATE FOR THE BUDGET AND THE MINISTER DELEGATE FOR SMALL AND MEDIUM-SIZED ENTERPRISES, INNOVATION AND THE DIGITAL ECONOMY 122 (2013), *available at* http://www.21stcenturytaxation.com/uploads/Taxation_Digital_Economy_Jan2013_France.pdf.

[66] *Id.* (emphasis omitted).

[67] *Id.* at 123.

[68] *Id.* ("The tax could take the form of a unit charge per user monitored. . . . The more 'compliant' the company's practices are regarding the collection, management and use of data derived from users' activity, the lower the unit charge would be. The charge could even be waived for the most compliant companies." (footnote omitted)).

become a tax on the export of data.[69] One report notes the possibility of "a global trade war taking place under the guise of taxation."[70]

Shortly after President François Hollande expressed outrage over U.S. spying, France adopted the Military Programming Law on December 10, 2013, dubbed by some "the French Patriot Act,"[71] permitting both the security forces and intelligence services from various ministries (defense, interior, economy, and budget)[72] to see "electronic and digital communications" in "real time."[73]

G. Germany

On July 24, 2013, in the wake of the NSA revelations, the Conference of the German Data Protection Commissioners announced that they would stop approving international data transfers until the German government could guarantee that foreign national intelligence services abide by fundamental principles of data protection law.[74] They relied on their authority from the

---

[69] The report accompanying the proposal suggests that compliance might mean going beyond complying with the letter of the law. *Id.* at 123–24 ("It is not yet time to determine which practices could be qualified as 'compliant' or 'non-compliant.' . . . The point is to assess whether, in addition to meeting its legal obligations, which it must do in any case, the company's approach goes above and beyond compliance with the letter of the law." (emphasis omitted)).

[70] Ian Allison, *Europe Cracks Down on Google, Apple, Facebook and the Data-Driven Tax Black Hole*, INT'L BUS. TIMES (Dec. 12, 2013, 09:18 GMT), http://www.ibtimes.co.uk/tax-internet-ec-oecd-google-facebook-apple-529601 (internal quotation marks omitted); *see also* Bruno Waterfield, *UK Braced for Battle with France over Google Data Tax*, TELEGRAPH (Oct. 23, 2013, 3:42 PM BST), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/10399840/UK-braced-for-battle-with-France-over-Google-data-tax.html.

[71] James Creedon, *Privacy Concerns After Passing of "French Patriot Act,"* FRANCE24 (Dec. 17, 2013), http://www.france24.com/en/20131212-french-patriot-act-military-programming-law-carla-bruni-nude-photos-hacking/.

[72] Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 on the Military Budget for the Years 2014–2019 and Miscellaneous Provisions for Defense and National Security], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 19, 2013, p. 20570 (Fr.); Kim Willsher, *French Officials Can Monitor Internet Users in Real Time Under New Law*, GUARDIAN (Dec. 11, 2013, 13:18 EST), http://www.theguardian.com/world/2013/dec/11/french-officials-internet-users-real-time-law.

[73] Willsher, supra note 72. The legislation has drawn criticism. Andréa Fradin, *L'article 13 Est-il Plus Dangereux pour Internet que les Lois Existantes?* [*Section 13: Is It More Dangerous for the Internet than Existing Laws?*], SLATE.FR (Dec. 17, 2013, 14h35), http://www.slate.fr/story/81011/loi-programmation-militaire-danger (Fr.) (critiquing the Association of Internet Community Services, Syntec, French Federation of Telecoms, MEDEF, International Federation of Human Rights, La Quadrature du Net, CNIL and the CNNum); *Alarm Over Massive Spying Provisions in New Military Programming Law*, REPORTERS WITHOUT BORDERS (Dec. 12, 2013), http://en.rsf.org/alarm-over-massive-spying-12-12-2013,45606.html.

[74] Press Release, Die Landesbeauftragte für Datenschutz und Informationsfreiheit [State Commissioner for Data Protection and Freedom of Information], Conference of Data Protection Commissioners Says that

Commission of the European Communities to suspend data transfers if either the Safe Harbor or the standard contractual clauses permitting data transfer have a "substantial likelihood" of violation.[75] The Commissioners argued that the violations arose because data transferred by German companies can be accessed by the NSA and various other foreign intelligence services without complying with limitation principles (viz., need, proportionality, and purpose).[76]

While the Commissioners sought to stop data flow outside Europe, some within Germany proposed to limit data flow only to routes within Germany. In October 2013, Deutsche Telekom (which is one-third state-owned)[77] proposed that data between Germans be routed inside German networks.[78] The idea was

---

Intelligence Services Constitute a Mass Threat to Data Traffic Between Germany and Countries Outside Europe (July 24, 2013), *available at* http://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.

[75] Commission Decision of 5 February 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5, 8 [hereinafter Commission Decision on Standard Contractual Clauses], *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF; *see also* Commission Decision of 27 December 2004 Amending Decision 2001/497/EC as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74, 74–75, *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF.

[76] German privacy regulators have taken issue with the Safe Harbor with the United States in the past. In 2010, German regulators, through an information organization known as the Düsseldorfer Kreises [Düsseldorf Circle], maintained that U.S. Safe Harbor self-certifications should not be automatically be considered as conclusive proof of adequate protection. *See* BESCHLUSS DER OBERSTEN AUFSICHTSBEHÖR DEN FÜR DEN DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH AM 28./29. APRIL 2010 IN HANNOVER, PRÜFUNG DER SELBST-ZERTIFIZIERUNG DES DATENIMPORTEURS NACH DEM SAFE HARBOR-ABKOMMEN DURCH DAS DATEN EXPORTIERENDE UNTERNEHMEN [DECISION OF THE BOARD OF SUPERVISORY AUTHORITIES FOR PROTECTION IN NON-PUBLIC AREAS ON 28/29TH APRIL 2010 IN HANNOVER, CONSIDERATION OF SELF-CERTIFICATION OF DATA IMPORTER TO THE SAFE HARBOR AGREEMENT BY THE DATA EXPORTING COMPANY] (Apr. 28, 2010), *available at* http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf;jsessionid=34480CBEFF09F90E0916CE90C8B0E224.1_cid354?__blob=publicationFile; *U.S.–EU Safe Harbor*, ELECTRONIC COM. & L. REP., June 23, 2010, at 1, *available at* http://www.willkie.com/~/media/Files/Publications/2010/06/German%20Authorities%20Issue%20Privacy%20Decision%20Clarif__/Files/German%20Authorities%20Issue%20Privacy%20Decision%20Clarif__/FileAttachment/German%20Authorities%20Issue%20Privacy%20Decision%20Clarif__.pdf; *German Privacy Regulators Issue Decision on Data Protection and Safe-harbor Self-Certification of US Companies*, DUANE MORRIS (June 1, 2010), http://www.duanemorris.com/alerts/Dusseldorfer_Kreis_Safe_Harbor_Privacy_3680.html. For a defense of the Safe Harbor, *see* Damon Greer, *Safe Harbor—A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 146 (2011).

[77] Cornelius Rahn & Tino Andresen, *Germany Should Sell 32% Deutsche Telekom Stake, Adviser Says*, BLOOMBERG (Dec. 16, 2013, 12:05 PM ET), http://www.bloomberg.com/news/2013-12-16/germany-should-sell-phone-stake-to-fund-networks-adviser-says.html.

[78] *Telecoms Plan Shielded European Internet*, DEUTSCHE WELLE (Nov. 10, 2013), http://www.dw.de/telecoms-plan-shielded-european-internet/a-17217304.

also supported by then-Interior Minister Hans-Peter Friedrich.[79] Earlier in August, Deutsche Telekom launched "E-mail made in Germany," a service that seeks to route data exclusively through domestic servers.[80] In February 2014, Chancellor Angela Merkel proposed that Europe build out its own internet infrastructure designed to keep data within Europe.[81] She believed that "European providers [could] offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic."[82] Some questioned whether the proposals, which would increase both network construction and operation costs significantly, would in fact protect data from foreign surveillance (an issue we return to in Part II.A below) or simply increase the profits of local network firms.[83]

H. India

In April 2011, the Indian Ministry of Communications and Technology published privacy rules implementing certain provisions of the Information Technology Act of 2000.[84] The "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules" limit the transfer of "sensitive personal data or information" abroad to two cases—when "necessary" or when the data subject consents to the transfer abroad.[85] Specifically, Rule 7 provides as follows:

---

[79] *See German Minister: Drop US Sites If You Fear Spying*, ASSOCIATED PRESS, July 3, 2013, *available at* http://bigstory.ap.org/article/german-minister-drop-google-if-you-fear-us-spying ("Whoever fears their communication is being intercepted in any way should use services that don't go through American servers . . . ." (internal quotation marks omitted)).

[80] *Will It Work? German Email Companies Adopt New Encryption to Foil NSA*, RT.COM (Aug. 11, 2013, 10:54), http://rt.com/news/german-email-encryption-nsa-312/.

[81] *Merkel and Hollande Mull Secure European Communication Web*, DEUTSCHE WELLE (Feb 16, 2014), http://www.dw.de/merkel-and-hollande-mull-secure-european-communication-web/a-17435895.

[82] *Id.* (internal quotation marks omitted).

[83] *Weighing a Schengen Zone for Europe's Internet Data*, DEUTSCHE WELLE (Feb. 20, 2014), http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482.

[84] The Information Technology Act 2000 focused on computer misuse but did not cover data security. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). The IT (Amendment) Act 2008 added two additional sections, Section 43A and Section 72A, to address the loss and protection of personal data. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

[85] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, subsection II(3)(i) (Apr. 11, 2011). The rules define the type of information that the Act covers:

> Sensitive personal data or information of a person means such personal information which consists of information relating to[:]—(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and

> A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.[86]

Because it is difficult to establish that a transfer data abroad is "necessary," this provision would effectively ban transfers abroad except when an individual consents.

The Rules, however, do not make it clear how consent for onward transfer from the information collector to the information processor is to be obtained. When it comes to collecting the personal information in the first instance, the rules require consent provided in writing, via fax, or through email—which (depending on how "writing" is interpreted) could foreclose even the typical webpage with an "I agree" button.[87] Commentators observed that the consent requirements were "far more restrictive" than what is required under United States or European Union laws.[88] European Union laws require consent for data collection and processing generally, not special consent for transfer abroad.[89] Special consent required for exporting data suggests that data sent to another country is, by that act, less safe—thus requiring special knowledge and approval of the data subject. Because consent for offshore transfer can be a significant practical hurdle, American critics of outsourcing to India have sought to impose a consent requirement before consumer information can be

---

> history; (vi) [b]iometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise[;] provided that, any information that is freely available or accessible in public domain or finished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Id. at Rule 3.

86 *Id.* at Rule 7.

87 MIRIAM H. WUGMEISTER & CYNTHIA J. RICH, MORRISON & FOERSTER, INDIA'S NEW PRIVACY REGULATIONS 3 (2011), *available at* http://www.mofo.com/files/Uploads/Images/110504-Indias-New-Privacy-Regulations.pdf.

88 *Id.* at 1.

89 Council Directive, *supra* note 45, at 40.

sent outside the United States.[90] As drafted, the Indian law seemed to ironically accomplish the goal of those against outsourcing to India—that is, requiring American companies to obtain the consent of individuals before passing their information to India.[91] In August 2011, the Ministry of Communications & Information Technology clarified that the Rules were meant only to apply to companies gathering data of Indians, and only where the companies were located in India.[92] While patching over one problem, the clarification may discourage foreign companies from investing in India because to do so would bring them under the purview of the Rules. (We return to the impact of data localization on local economic development in Part II.C below.)

Another statute potentially poses substantial localization pressures for information held by the government. Section 4 of the Public Records Act of 1993 prohibits public records from being transferred out of India territory, except for "public purpose[s]."[93] It provides that "[n]o person shall take or cause to be taken out of India any public records without the prior approval of the Central Government; [p]rovided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose."[94]

Under the statute, "any . . . material produced by a computer" constitutes "public records."[95] In 2013, the Delhi High Court interpreted this requirement to bar the transfer of government emails outside India.[96] It ordered the

---

[90] A bill proposed in New York explicitly designed to "stem the flow of skilled and unskilled labor out of New York State" requires that no business transfer "personal information to or with any nonaffiliated third parties which are located outside the United States . . . without . . . prior written consent." New York Consumer and Worker Protection Act, S. 2992, 2013 Reg. Sess. (N.Y. 2013).

[91] James A Harvey & Todd S. McClelland, *Outsourcing and Privacy & Security Advisory—Questions Answered, More Questions Raised: Exploring the Outsourcing Implications of India's Recently Released Privacy Rules*, ALSTON & BIRD LLP (June 21, 2011), http://www.alston.com/files/publication/34af0cc7-3ec9-4c05-b713-3692f2addf28/presentation/publicationattachment/9a608746-920d-4990-8b2b-57ef0e1a8b76/outsourcing%20and%20privacy%20%26%20security%20advisory.pdf.

[92] *See* Press Note, Press Info. Bureau, Gov't of India, Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000, (Aug. 24, 2011), *available at* http://pib.nic.in/newsite/erelease.aspx?relid=74990; Deepa Christopher & Praveen Thomas, *India – Welcome Clarification on Sensitive Personal Data Rules*, LINKLATERS (Sept. 20, 2011), http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-newsletter-September-2011/Pages/India-data-security-laws.aspx.

[93] The Public Records Act, No. 69 of 1993, § 4, INDIA CODE (1993), *available at* http://nationalarchives.nic.in/writereaddata/html_en_files/html/public_records93.html.

[94] *Id.*

[95] *Id.* § 2(e)(iv).

[96] *See Delhi HC Asks Government to Formulate an Email Policy Within 4-weeks*, IBN LIVE (Oct. 30, 2013, 3:06 PM IST), http://ibnlive.in.com/news/delhi-hc-asks-government-to-formulate-an-email-policy-

government to formulate a policy for official government email that would comply with the Public Records Act.[97] A draft of the "E-mail Policy of the Government of India" would mandate that government employees use only government email services, thereby preventing the use of private services based abroad or at home.[98] The Information Technology Directorate of the state of Maharashtra advised all government department's websites "should be hosted within India and preferably on government owned servers" and to use "government provided email IDs, from servers within India . . . for official communication by all government employees."[99]

In February 2014, the National Security Council (NSC) proposed a policy that might require data localization for Indian citizens, and not just government agencies alone. According to an NSC internal note seen by the newspaper *The Hindu Business Line*, "All email service providers may be mandated to host servers for their India operations in India. All data generated from within India should be hosted in these India-based servers and this would make them subject to Indian laws[.]"[100] The NSC proposal would prohibit "[a]s a general principle, mirroring of data in these servers to main servers abroad."[101]

Moreover, the National Security Advisor has called on the Department of Telecom to mandate all telecom and Internet companies "to route local data through the National Internet Exchange of India" to ensure that domestic Internet packets remain mostly in India.[102] The Standing Committee on Information Technology of the Ministry of Information noted in February 2014 that it is "unhappy" that a "majority of the websites are still being hosted outside India."[103]

---

within-4weeks/431351-3-244.html; *see also Delhi High Court Seeks Clear-cut Answers from Centre on Its Email Policy*, ECON. TIMES (Oct. 1, 2014, 07:19 PM IST), http://articles.economictimes.indiatimes.com/2014-10-01/news/54516892_1_email-policy-k-n-govindacharya-delhi-high-court.

97 *Delhi HC Asks Government to Formulate an Email Policy within 4-weeks*, *supra* note 96.

98 STANDING COMMITTEE ON INFORMATION TECHNOLOGY, CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY 21 (2014), *available at* https://www.dsci.in/sites/default/files/15_Information_Technology_52.pdf.

99 Letter from Rajesh Aggarwal, Sec'y of Info. Tech., Directorate of Info. Tech., to all Gov. Depts. in Maharashtra, India 2 (Sept. 30, 2013), *available at* https://www.maharashtra.gov.in/Site/upload/WhatsNew/Advisory%20dated%20300913.pdf.

100 Thomas K. Thomas, *National Security Council Proposes 3-Pronged Plan to Protect Internet Users*, HINDU BUS. LINE (Feb. 13, 2014), http://www.thehindubusinessline.com/features/smartbuy/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece (internal quotation marks omitted).

101 *Id.*

102 Thomas, *supra* note 3.

103 STANDING COMMITTEE ON INFORMATION TECHNOLOGY, *supra* note 96, at 61.

I. Indonesia

In 2012, the Indonesian government required service providers providing "public services" to place their data centers within the country. Regulation 82 concerning "Electronic System and Transaction Operation" states, "Electronic System Operator for the public service is obligated to put the data center and disaster recovery center in Indonesian territory for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens."[104] Although the term "public services" is defined in the Public Service Law of 2009,[105] this provision did not define exactly what kinds of "electronic system operators" were deemed to be in the "public service."[106] A Draft Regulation Concerning Registration Procedure of Electronic System Provider clarifies this somewhat, explaining that "public service electronic systems by the private business sector" include any "[o]nline gate, site or online application over the internet which provides an offer and/or trade of goods and/or service; . . . enables payment facility and/or other financial transaction over the data network; . . . [or] is used for paid digital content delivery over the data network."[107]

On its face, this approach seems so broad that almost all websites and online applications such as newspapers or information and social platforms

---

[104] Regulation Concerning Electronic System and Transaction Operation, Law No. 82 of 2012, art. 17(2) (Government Gazette of the Republic of Indonesia Year 2012 No. 189) (Indon.), *translation available at* TECHNICAL COOPERATION PROJECT FOR CAPACITY DEVELOPMENT FOR TRADE-RELATED ADMINISTRATION IN INDONESIA, http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html. The Regulation serves to clarify the Law on Information and Electronic Transactions 2008.

[105] Undang-Undang Tentang Pelayanan Publik [Public Service Law], Law No. 25/2009, July 18, 2009 (Government Gazette of the Republic of Indonesia Year 2009 No. 112) (Indon.), *available at* http://www.setneg.go.id//components/com_perundangan/docviewer.php?id=2274&filename=UU%2025%20Tahun%202009.pdf; *see also* Michael Buehler, *Indonesia's Law on Public Services: Changing State-Society Relations or Continuing Politics as Usual?*, 47 BULL. INDON. ECON. STUD. 65 (2011), *available at* http://michaelbuehler.asia/wp-content/uploads/2012/06/BIESBuehler2011.pdf.

[106] Law No. 25/2009, art. 5.7(b); *Indonesia, Transfer of Personal Data to Third Countries*, LINKLATERS, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Indonesia.aspx (last updated May 2014). Public services are services (a) provided by government agencies, (b) provided by a business entity founding capital partly or entirely derived from the wealth of the country, (c) provided by none of the above but whose delivery is part of state's mission. In the elucidation, it was further stated that the State's missions are: health, education, inter city transportation, aviation, social welfare homes, and security services. *See Indonesia, Transfer of Personal Data to Third Countries*, *supra*.

[107] Rancangan Peraturan Menteri (RPM) tentang Tata Cara Pendaftaran Penyelenggaraan dan Sistem Transaksi Elektronik [Draft Regulation Concerning the Registration Procedure of Electronic System Provider], art. 5, http://web.kominfo.go.id/sites/default/files/RPM%20tentang%20Tata%20Cara%20Pendaftaran%20Penyelenggara%20Sistem%20Elektronik.pdf (Indon.) (Pricillia Haesanny, trans., translation on file with authors).

might be "public services" because, due to the nature of service-bundling, these sites also often process paid digital content or offer other services. The Indonesian Association of E-commerce (idEA) has criticized this interpretation as inconsistent with regulations on public services.[108]

On January 7, 2014, the Ministry of Communication circulated a Draft Regulation on Technical Guidelines on Data Centers, which would require domestic data centers for disaster recovery for a broader range of institutions.[109] According to the Technology and Information Ministry's Chief of Public Relations Gatot S. Dewa Broto, the local data center mandate "covers any institution that provides information technology-based services," which as a prescient reporter noted, is a definition which is broad enough that it could include "hotels, banks, and airlines services as well as [Google and Yahoo]."[110] As we'll describe in Part II.C below, the costs and risks associated with building out data centers in every country that one serves can make it uneconomical to do so in many cases.

J. Malaysia

In 2010, Malaysia passed the Personal Data Protection Act (PDPA), which requires data about Malaysians to be stored on local servers.[111] Article 129(1) provides, "A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the *Gazette*."[112] The PDPA offers a set of exceptions, permitting the transfer of data abroad under certain conditions: the data subject has given his consent to the transfer; the transfer is necessary for the performance of a contract between

---

[108] Enricko Lukman, *Is the Indonesian Government Hurting or Helping the E-Commerce Industry?*, TECH IN ASIA (May 9, 2013, 5:12 PM), http://www.techinasia.com/indonesian-government-hurting-helping-ecommerce-industry/.

[109] Rancangan Peraturan Menteri (RPM) tentang Pedoman Teknis Pusat Data [Draft Regulation Concerning the Technical Guidelines for Data Centers] (2013) (Indon.), *available at* http://web.kominfo.go.id/sites/default/files/RPM%20PEDOMAN%20PUSAT%20DATA.pdf; Press Release, Kominfo, Siaran Pers Tentang Uji Publik RPM Data Center [Press Release About Public Test RPM Data Center] (Jan. 7, 2014) (Indon.), *available at* http://kominfo.go.id/index.php/content/detail/3731/Siaran+Pers+No.+2-PIH-KOMINFO-1-2014+tentang+Uji+Publik+RPM+Data+Center+/0/siaran_pers#.UxBPWvldV6B.

[110] *Indonesia May Force Web Giants to Build Local Data Centers*, ASIA SENTINEL (Jan. 17, 2014), http://www.asiasentinel.com/econ-business/indonesia-web-giants-local-data-centers/; *see also* Vanesha Manuturi & Basten Gokkon, *Web Giants to Build Data Centers in Indonesia?*, JAKARTA GLOBE (Jan. 15, 2014, 9:35 AM), http://www.thejakartaglobe.com/news/web-giants-to-build-data-centers/.

[111] Personal Data Protection Act 2010 § 129 (Act No. 709) (Malay.), *available at* http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.

[112] *Id.* art. 129(1).

the data subject and the data user; the transfer is necessary for the conclusion or performance of a contract between the data user and a third party that is either entered into at the request of the data subject or in his interest; the transfer is in the exercise of or to defend a legal right; the transfer mitigates adverse actions against the data subjects; reasonable precautions and all due diligence to ensure compliance to conditions of the Act were taken; or the transfer was necessary for the protection the data subject's vital interests or for the public interest as determined by the Minister.[113] As we have indicated above in our discussion of the Indian data localization obligations, a consent requirement for transfer abroad can be difficult to satisfy. While it officially entered into force on November 15, 2013, the PDPA has thus far not been enforced.

K. Nigeria

To address Nigeria's "clear negative trade balance" in the IT sector, the Nigerian government has set a target of 50% locally supplied goods and services in the information technology sector and has sought to achieve this target through regulatory mandates.[114] The National Information Technology Development Agency (NITDA) released the Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) in 2013, requiring, in addition to a list of local content and usage of local hardware requirements, that ICT companies must "[h]ost all subscriber and consumer data locally within the country"[115] and must "[h]ost their websites on .ng TLD."[116] The Guidelines also mandate that data and information management firms must "[h]ost government data locally within the country and shall not for any reason host any government data outside the country without an express approval."[117] The Guidelines provide a transition period for implementation.[118]

---

[113] *Id.* art. 129(3).

[114] Omobola Johnson, Minister of Commc'n Tech., Federal Ministry of Commc'n Tech., Remarks at the e-Nigeria Conference 2013 in Abuja, Nigeria (Dec. 3, 2013), *available at* http://enigeria.gov.ng/2013/Day%201/HM%20Remarks_e_Nigeria%20Dec%2003rd%202013_v5a.pdf.

[115] Federal Ministry of Commc'n Tech., Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) § 12.1.4, at 19 (2013), *available at* http://www.nitda.gov.ng/documents/Guidelines%20on%20Nigerian%20Content%20Developmenet%20in%20ICT%20updated%20on%2012062014.pdf.

[116] *Id.* § 12.1.5, at 19.

[117] *Id.* § 14.1.2, at 23.

[118] *See id.* § 1.0, at 4.

L. Russia

Following the NSA revelations in the summer of 2013, Sergei Zheleznyak, a deputy speaker of the lower house of the Russian parliament and a member of the Committee on Information Policy and Information Technology and Communications, called on Russia to strengthen its "digital sovereignty" through "legislation requiring e-mail and social networking companies [to] retain the data of Russian clients on servers inside Russia, where they would be subject to domestic law enforcement search warrants."[119]

In spring 2013, the *Minsvyazi* (Russian Ministry of Communications) drafted an order forcing telecommunications and Internet providers "to install equipment allowing data collection and retention on their servers for a minimum of 12 hours."[120] This obligation seems to be directed not at the websites themselves but at Internet service providers that carry data between users and computer servers. By requiring Russian Internet service providers to save data locally, it serves as a data localization requirement, not preventing data from leaving but at least requiring a copy to be stored locally. This order gives the Russian Federal Security Service (FSB) "direct access to a wider range of data than was possible before—including users' phone numbers, account details on popular domestic and overseas online resources (like Gmail, Yandex, Mail.ru etc [sic]), IP addresses and location data—without a court order, for the purposes of national anti-terrorist investigations."[121] On July 21, 2014, President Vladimir Putin signed Federal Law No. 242—which amended Federal Law No. 152 "On Personal Data" of July 27, 2006[122]—to prohibit the storing of Russians' personal data outside the Russian Federation.[123] Moreover,

---

[119] Andrew E. Kramer, *N.S.A. Leaks Revive Push in Russia to Control Net*, N.Y. TIMES, July 15, 2013, at B1, *available at* http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html; Maria Makutina, *Lawmakers Seek to Bolster Russia's Internet Sovereignty*, RUSS. BEYOND HEADLINES (June 21, 2013), http://rbth.ru/politics/2013/06/21/lawmakers_seek_to_bolster_russias_internet_sovereignty_27365.html.

[120] Alexandra Kulikova, *Data Collection and Retention in Russia: Going Beyond the Privacy and Security Debate*, GLOBAL PARTNERS DIGITAL (Jan. 17, 2014), http://www.gp-digital.org/gpd-update/data-collection-and-retention-in-russia/.

[121] *Id.*

[122] Federal'nyi Zakon RF o Personal'nykh Data [Federal Law of the Russian Federation on Personal Data], ROSSIISKAIA GAZETA [ROS. GAZ.] July 27, 2006, No. 152, *available at* http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, *translation available at* https://www.privacyassociation.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf (Int'l Ass'n of Privacy Prof'ls, trans.).

[123] Federal'nyj Zakon Rossijskoj Federacii "O Vnesenii Izmenenij v Otdel'nye Zakonodatel'nye Akty Rossijskoj Federacii v Časti Utočnenija Porjadka Obrabotki Personal'nyh Dannyh v Informacionno-Telekommunikacionnyh Setjah" [Federal Law of the Russian Federation "On Amendments to Certain

operators of these databases must disclose the physical locations of datacenters.[124] Online websites that violate the prohibition could be placed on the *Roscomnadzor*'s (Federal Communications Supervisory Service's) blacklist of websites, generally reserved for those promoting drugs and child pornography.[125]

This law followed on the heels of Federal Law No. 97, or the "Blogger's Law," which seeks to oversee blogging on the Internet, and introduces another data localization mandate.[126] The legislation requires that individuals or legal entities who organize the dissemination of information, or the exchange of information between Internet users, to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action for six months in Russia.[127] A major firm noted that these "[t]wo developments in Russian law . . . could significantly limit the ability of cloud and other online services to publish online content and to make Russian data remotely available online."[128]

Legislative Acts of the Russian Federation Regarding the Clarification of the Processing of Personal Data in Information and Telecommunication Networks"], ROSSIISKAIA GAZETA [ROS. GAZ.] July 23, 2014, No. 242, *available at* http://www.rg.ru/2014/07/23/persdannye-dok.html; *see also* Maria Puzrakova, *Recent Amendments to the Procedure of Personal Data Processing in Russia*, WHITE & CASE LLP (Sept. 2014), http://www.whitecase.com/articles/092014/recent-amendments-to-the-procedure-of-personal-data-processing-in-russia/#.VEl-NskhCkM; Leonid Zubarev & Elena Baryshnikova, *The Storage and Processing of Russian Citizens' Personal Data in Databases Located Outside Russia to be Banned*, CMS (Aug. 2014), http://www.cms-russia.info/legalnews/2014/07/cms_client_alert_2014_07_31.html (explaining Russian citizens' personal data will only be stored on Russian Databases and noting exceptions such as when there is interference to achieving objectives of international treaties and the administration of justice).

124 Federal Amendments to Certain Legislative Acts of the Russian Federation, art. 2.2.

125 Max Smolaks, *Russian Government Will Force Companies to Store Citizen Data Locally*, TECHWEEK EUROPE (July 4, 2014, 17:22), http://www.techweekeurope.co.uk/news/russian-government-will-force-companies-store-citizen-data-locally-148560.

126 Federal'nyj Zakon "O Vnesenii Izmenenij v Federal'nyj zakon, 'Ob Informacii, Informacionnyh Tehnologijah i o Zaŝite Informacii' i Otdel'nye Zakonodatel'nye akty Rossijskoj Federacii po Voprosam Uporjadočenija Obmena Informaciej s Ispol'zovaniem Informacionno-Telekommunikacionnyh Setej" [Federal Law "On Amending the Federal Law 'On Information, Information Technologies and Protection of Information' and Certain Legislative Acts of the Russian Federation on Streaming the Exchange of Information with the Use of Information-Telecommunications Networks"], ROSSIISKAIA GAZETA [ROS. GAZ.] May 5, 2014, art. 1.1, *available at* http://www.rg.ru/2014/05/07/informtech-dok.html. For a general overview of the regulation, see Natalia Gulyaeva & Maria Sedykh, *Russia Enacts Data Localization Requirement; New Rules Restricting Online Content Come into Effect*, HOGAN LOVELLS (July 18, 2014), http://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/.

127 *See* Federal Law of May 5, 2014, art. 1.1; *see also Russia's Parliament Prepares New "Anti-Terrorist" Laws for Internet*, GLOBAL VOICES (Jan. 16, 2014, 5:51 GMT), http://advocacy.globalvoicesonline.org/2014/01/16/russias-parliament-prepares-new-anti-terrorist-laws-for-internet-censorship-putin/.

128 Gulyaeva & Sedykh, *supra* note 126.

M. South Korea

In March 2011, South Korea promulgated a comprehensive regulation on data through the Personal Information Protection Act, covering both the private and public sectors.[129] Article 17(3) of the Act targets data exports for a special protection regime: "When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to . . . and obtain the consent thereto."[130]

The law requires the data exporter to provide the data subject (the person to whom the data relates) with extensive information about the data transfer. Article 17(2) provides that data subjects must be informed of the following:

> 1. A recipient of personal information; 2. Purposes for which a recipient of personal information uses such information; 3. Items of personal information to provide; 4. Period for which a recipient of personal information holds and uses such information; 5. The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent.[131]

As we described in the discussion of similar rules in India, these obligations significantly limit the use of foreign cloud computing services and also third party information services providers generally.

Another data localization measure comes from an unexpected source. In 1961, post-war South Korea enacted the Land Survey Act seeking, among other things, to prevent hostile powers from obtaining maps of the country.[132] Similar provisions were replaced in 2009 by the Act on Land Survey,

---

[129] Gaein jeong boboho beop [Personal Information Protection Act], Act. No. 10465, Mar. 29, 2011, art 1, *amended by* Act. No. 11690, Mar. 23, 2013 (S. Kor.), *translated in* 33 STATUTES OF THE REPUBLIC OF KOREA (Korea Legislation Res. Inst. 2014), *available at* http://elaw.klri.re.kr/eng_service/lawView.do?hseq=22038&lang=ENG. The Personal Information Protection Act replaced the Public Agency Data Protection Act and—in part in relation to the private sector—the Act on Promotion of Information and Communications Network Utilization and Information Protection.

[130] *Id.* art. 17(3).

[131] *Id.* art. 17(2).

[132] Land Survey Act, Act. No. 938, Dec. 31, 1961, art. 16 (forbidding records of survey measurements and pictures of maps from being taken out of the country), *repealed by* Act on Land Survey, Waterway Survey and Cadastral Records, Act. No. 9774, June 9, 2009 (S. Kor.). For the current version of the law in force, *see* Act on Land Survey, Waterway Survey and Cadastral Records, Act. No. 12738, June 3, 2014 (S. Kor.), *translated in* 31 STATUTES OF THE REPUBLIC OF KOREA (Korea Legislation Res. Inst. 2014), *available at* http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG.

Waterway Survey and Cadastral Records, which has been amended several times, most recently in 2014. According to Article 16 of the Act,

> (1) No person shall take abroad maps, etc. . . . without permission of the Minster of Land, Transport and Maritime Affairs . . .
>
> (2) No person shall take abroad the results of a fundamental survey where [the act would harm national security or other important national interests or where such information is prescribed as a confidential matter].[133]

The constraint in this law continues to this day,[134] and it has been interpreted recently as outlawing mapping data from being held on computer servers outside the country.[135] This has effectively limited the provision of online mapping services to Korean Internet companies such as Naver and Daum and not foreign companies that use foreign servers. A Japanese tourist, for example, found that she could not use Google Maps to navigate in South Korea.[136] The constraints also pose a hurdle to companies that provide services built on top of the foreign services' APIs (application programming interfaces), thereby hampering the development of domestic innovations using global tools, an issue we return to in Part II.C below.

N. Vietnam

In 2013, the Vietnamese government promulgated a lengthy and comprehensive decree seeking to control speech on the Internet. The Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72),[137] which became effective on September 1, 2013, bans the use of the Internet to criticize the government or to do anything else to harm "national security, social order and safety."[138] Decree 72 also requires a range of Internet service providers to maintain within Vietnam a copy of any

---

[133] Act. No. 12738, June 3, 2014, art. 16 (concerning the results from a "fundamental survey"); *see also id.* art. 21 (concerning the results from a "public survey").

[134] *See supra* note 133.

[135] *See* Geun Ho LiIm, Hangyeong → Seouryeok Geomsaek Haessdeoni. . .Geonmul Wiro Naragarago? Hangug Eseoman Gil Moschajneun Gugeuljido [*Searching Directions from HanKyung to Seoul Station. . .Fly over Buildings? Google Map Cannot Navigate only in Korea*], KOREA ECON. DAILY (Dec. 9, 2013, 21:10:50), http://www.hankyung.com/news/app/newsview.php?aid=2013120998951 (S. Kor.).

[136] *Id.*

[137] Decree on Management, Provision and Use of Internet Services and Online Information (No. 72/2013) (Viet.), *available at* http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf.

[138] *Id.* art. 5(1)(a) (declaring it illegal to use the Internet to "[oppose] the Socialist Republic of Vietnam [or] threaten[] the national security, social order and safety").

information they hold in order to facilitate the inspection of information by authorities, specifically, providing that organizations and enterprises must "have at least [one] server system in Vietnam serving the inspection, storage, and provision of information at the request of competent authorities."[139]

The Decree applies to general websites, social networks, mobile networks, and game service providers.[140] Unlike many other countries, Vietnam's focus is not in protecting the privacy of the information from foreign surveillance but in ensuring that information is available to local authorities that want ready access to it.

In October 2013, the Ministry of Information and Communications circulated a draft circular providing additional implementation details for Decree 72. The draft circular again affirms that a central goal of that decree is to assist local authorities in accessing information. The draft circular requires that the local server must meet the following requirements:

> 1. Storing all user registration information that allows users to connect and authenticate user information with personal identification number system at the request of the competent state agencies.
>
> 2. Storing the entire history of the information posting activities on the general information websites and user information provision and sharing on social networks.
>
> 3. Allowing the conduct and storage of all the activities relating to censoring information posted on general information websites and social networks.
>
> 4. When there are requirements arising from the server system located in Viet Nam, the entire server system located outside Viet Nam must meet those requirements.
>
> 5. Permitting full conduct of inspection and examination activities at any given time as required by the competent authority as well as the settlement of users' complaints in accordance with the user agreements of general information websites, social networks, and relevant regulations.[141]

---

[139] *Id.* art. 24(2).

[140] *See id.* (general websites); *id.* art. 25(8) (social networks); *id.* art. 28(2) (mobile networks); *id.* art. 34(2) (game service providers).

[141] Draft Circular Detailing a Number of Articles re Management of Websites and Social Networks under the Government's Decree No. 72/2013/ND-CP of 15 July 2013 Regarding the Management, Provision and Use

The draft circular also requires that any "general information website" or social network must have a high-level person responsible for content management who must be a Vietnamese national and reside in Vietnam.[142] Thus, not only must the data reside in Vietnam, so must a high-level executive of the company.

O. Others

Kazakhstan—Since 2005, Kazakhstan has required that all domestically registered domain names (i.e., those on the ".kz" top level domain) operate on physical servers within the country.[143] The government took steps to enforce this regulation in late 2010, causing Google to redirect traffic from Google.kz to Google.com.[144] The redirect caused search queries to return results that were not customized for Kazakhstan.[145] The Kazakhstani Association of IT Companies later required that the domestic server requirements apply only to new domains registered after September 7, 2010.[146] This allowed Google (which had registered its name well before this date) to restore the Google.kz site, but domestic or foreign companies registering a domain name after this date could no longer rely on global cloud-based services.

Scandinavian Countries—The Scandinavian data protection authorities have expressed concerns about the use of foreign cloud computing services,

---

of Internet Services and Online Information, Vietnamese Ministry of Information and Communication, *available at* http://mic.gov.vn/Attachment%20Lay%20Y%20Kien%20Nhan%20Dan/Du%20thao%20thong%20tu%20MXH%20(Du%20thao%203%20ngay%204.%209).doc (translation by author).

142 *Id.* art. 3. This provision sets forth conditions for granting a license to establish general information websites and social networks, which include the following specifications:

> 1. Management personnel:
>
> The person responsible for content management is the head of the organization, the head of the enterprise or the person who is authorized by the head of an organization, the head of an enterprise. The authorized person must be deputy head-level in an organization and an enterprise; must have Vietnamese nationality, permanent residence or temporary residence address in Vietnam, and must be an university graduate or equivalents or higher . . . .

Id.

143 FREEDOM HOUSE, *supra* note 8, at 441.

144 Bill Coughran, *Changes to the Open Internet in Kazakhstan*, GOOGLE OFFICIAL BLOG (June 14, 2011, 7:40 PM), http://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html ("[T]he Kazakhstan Network Information Centre notified us of an order issued by the Ministry of Communications and Information in Kazakhstan that requires all .kz domain names, such as google.kz, to operate on physical servers within the borders of that country.").

145 *Id.*

146 *See id.*; *see also Google.kz Vernulsya v Kazakhstan* [*Google.kz Returned to Kazakhstan*], TENGRINEWS.KZ (June 15, 2011, 10:20), http://tengrinews.kz/internet/190571/ (Kaz.).

though their interpretations have been largely untested in court. In 2011, the Danish Data Protection Agency denied the city of Odense permission to transfer "data concerning health, serious social problems, and other purely private matters" to Google Apps, citing security concerns.[147] In 2012, the Norwegian data authority concluded that cities could not use cloud computing services unless the servers were located within the EU, but then lifted the ban on the use of Google Apps a short time later.[148]

Sweden's *Datainspektionen* (Data Inspection Board) has given a number of interpretations on whether the use of services that place data abroad violates Swedish data processing law. It concluded that the town of Salem could not use Google cloud services, in part because Google could not guarantee that any subcontractor they used abroad would follow the Safe Harbor.[149] Google's standard enterprise contract, however, promises that any subcontractor will meet the standards of the Safe Harbor, and Google also provides for the possibility that it will follow the Model Contract Clauses established by the European Commission to meet the requirements of European data protection law.[150] The *Datainspektionen* did eventually approve the use of Dropbox, a U.S.-based cloud service.[151]

---

147 *Processing of Sensitive Personal Data in a Cloud Solution*, DATATILSYNET (Feb. 3, 2011), http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/.

148 *See* Norwegian Data Inspectorate, *Notification of Decision – New E-mail Solution Within Narvik Local Authority (Narvik Commune) – Google Apps*, DATATILSYNET (Jan. 16, 2012), http://www.datatilsynet.no/Global/english/2012_narvik_google_eng.pdf (decision to ban service); *Use of Cloud Computing Services*, DATATILSYNET (Sept. 26, 2012), http://www.datatilsynet.no/English/Publications/cloud-computing/ (reporting on the decision to lift the ban); *see also* Loek Essers, *Norway Ends Nine-Month Ban on Google Apps*, COMPUTERWORLD (Sept. 26, 2012, 2:27 PM PT), http://www.computerworld.com/article/2491685/cloud-computing/norway-ends-nine-month-ban-on-google-apps-use.html.

149 Dan Jerker B. Svantesson, *Data Protection in Cloud Computing – The Swedish Perspective*, 28 COMPUTER L. & SECURITY REV. 476, 476–77 (2012); *Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011* [*Supervision Under the Personal Data Act (1998: 204) – Monitoring of Decision in Case 263-2011*], DATAINSPEKTIONEN (May 31, 2013), http://www.datainspektionen.se/Documents/beslut/2013-05-31-salems-kommun.pdf (Swed.); Liam Tung, *Sweden Tells Council to Stop Using Google Apps*, ZDNET (June 14, 2013, 13:46 GMT), http://www.zdnet.com/sweden-tells-council-to-stop-using-google-apps-7000016850/. Also, in 2013, the *Datainspektionen* refused to endorse the Sollentuna municipality's cloud service contract with Google, though that interpretation too is being contested. *See* Jonas Ryberg, *Storbråk om Google Apps* [*Large Fraction of Google Apps*], COMPUTERSWEDEN (Sept. 17, 2013, 09:45), http://computersweden.idg.se/2.2683/1.523293/storbrak-om-google-apps (Swed.).

150 *Data Processing Amendment to Google Apps Enterprise Agreement*, GOOGLE, https://www.google.com/intx/en/enterprise/apps/terms/dpa_terms.html (last visited Feb. 6, 2015). The Model Contract Clauses provide for "prior written consent" before the use of subprocessors by the data importer. *See* Commission Decision on Standard Contractual Clauses, *supra* note 75.

151 Svantesson, *supra* note 149, at 479.

Taiwan—Article 21 of Taiwan's Personal Data Protection Act[152] permits government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions such as when the information involves major national interests, by treaty or agreement, inadequate protection, or when the foreign transfer is utilized to avoid Taiwanese laws.[153]

Thailand—Thailand is considering a comprehensive data protection framework.[154] The draft Personal Information Protection Act would require that before an overseas data transfer is executed, the data subjects must give specific consent in writing to overseas transfers, and the recipient country's personal data protection law must be deemed adequate.[155]

P. Summary of Data Localization Mandates

We summarize below the means employed and rationales offered for the data localization mandates that are in place or being considered in the jurisdictions surveyed.

Country	Regulation	Rationale Cited
Australia	Section 77 of the Personally Controlled Electronic Health Records (PCEHR) Act prohibits the transfer of health records outside of Australia.	Users' privacy and security

[152] Taiwan passed the Computer-Processed Personal Data Protection Law (CPPDP) and associated rules in 1995. In 2010, the CPPDP was amended and renamed the Personal Information Protection Act (PIPA). PIPA came into effect on October 1, 2012.

[153] Personal Information Protection Act (promulgated by the Ministry of Justice, May 26, 2010), art. 21 (Taiwan), *available at* http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021. The act provides for the following exceptions:

> 1. Where it involves major national interests; 2. Where [a] national treaty or agreement specifies otherwise; 3. Where the country receiving personal information lacks of proper regulations towards the protection of personal information and it might harm the rights and interests of the Party; 4. Where international transmission of personal information is made through an indirect method in which the provisions of this Law may not be applicable.

Id. Taiwan's National Communications Commission issued an order prohibiting all Taiwanese telecommunications and broadcasting industries from transferring customer data to the People's Republic of China, citing reasons of inadequate protection. *See* Ken-Ying Tseng & Rebecca Hsiao, *Taiwan*, *in* GETTING THE DEAL THROUGH: DATA PROTECTION & PRIVACY IN 26 JURISDICTIONS WORLDWIDE 2014, at 166 (2014), *available at* http://www.leeandli.com/dl.aspx?filecode=1728.

[154] Phrarāchbaronal trûmkhrxng k̂hxmūl s̄wn bukhkhl [Personal Data Protection Act] (Tentative Draft, 2012) (Thai.), *translation available at* http://media.mofo.com/docs/mofoprivacy/Thai%20data%20protection%20bill.doc.

[155] *Id.* § 16.

Country	Regulation	Rationale Cited
Brazil	A draft Marco Civil Proposal would have permitted the Executive branch to require Internet providers to use local structure for storage and dissemination of data.	Users' privacy and security, foreign surveillance[156]
Canada (British Columbia & Nova Scotia)	Laws requiring personal information held by public bodies to be stored and accessed only in Canada unless certain exceptions apply.	Foreign surveillance[157]
China	The People's Bank of China prohibits financial institutions from storing or processing personal information relating to identity, property, account, credit, and financial transactions outside of China.	Users' privacy and security
	The Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information System (the Guidelines) prohibit the transfer of personal data abroad without express consent of the data subject or explicit regulatory approval.	Users' privacy and security[158]
	The Law of the People's Republic of China on Guarding State Secrets prohibits data deemed states secrets from being transferred outside of China.	National security, foreign surveillance
European Union	The European Union's 1995 Data Protection Directive permits transfer of personal data if another jurisdiction provides adequate protection, there is a contractual arrangement with foreign company or through the Safe Harbor.	Users' privacy and security

156 Statement by Dilma Rousseff, *supra* note 20.
157 CATE, *supra* note 26.
158 *See supra* notes 38–41 and accompanying text.

Country	Regulation	Rationale Cited
European Union (continued)	The proposed General Data Protection Regulation permits the transfer of data outside European Union if there are appropriate safeguards such as binding corporate rules, valid European Data Protection Seal for both controllers and recipients, standard data protection clauses, or contractual clauses authorized by a state data protection authority.	Users' privacy and security
France	Proposed to tax the collection, management, and commercial exploitation of personal data generated by users located in France.	Users' privacy and security; economic development[159]
	The Military Programming Law permits security forces and intelligence services to see electronic and digital communications in real time.	National security, foreign surveillance
Germany	The Conference of German Data Protection Commissioners suspended personal international data transfer approvals upon determining that the Safe Harbor and the standard contractual clauses have a "substantial likelihood" of violations.	Foreign surveillance[160]
	Deutsche Telekom proposed that data between Germans should be routed inside German networks. Chancellor Angela Merkel supported this proposal and promoted the expansion of the concept to the European Union.	Users' privacy and security, foreign surveillance[161]
India	The Information Technology Rules prohibit the transfer of "sensitive personal data or information" abroad unless the data subject consented to the transfer or the transfer is "necessary."	National security

159 COLLIN & COLIN, *supra* note 65.
160 *See supra* note 75 and accompanying text.
161 *See supra* notes 77–83.

Country	Regulation	Rationale Cited
India (continued)	The Public Records Act of 1993 prohibits public records from being transferred out of Indian territory, except for public purposes. The Act barred the transfer of government emails outside of India.	National security, foreign surveillance
	The National Security Council proposes (1) that email service providers must host servers in India, (2) data generated from within India must be hosted in India, and (3) that mirroring of data to servers abroad is prohibited.	National security[162]
Indonesia	Regulation 82 on the Operation of Electronic System and Transaction Operation requires public service providers to place data centers within the country.	Law enforcement, national sovereignty, user's security
	Draft Regulation on Technical Guidelines on Data Center requires any institutions that provide information technology-based services to build local disaster recovery data centers.	Users' security
Malaysia	The Personal Data Protection Act prohibits the transfer of personal data abroad unless specified by the Minister or subjected to certain exceptions including the consent and "necessity" requirements.	Users' privacy and security[163]
Nigeria	Nigeria National Information Technology Development Agency's Guidelines for Nigerian Content Development in Information and Communications Technology require ICT companies to host all consumer and government data locally within the country.	Economic development[164]

[162] *See supra* notes 100–03 and accompanying text.

[163] Datuk Seri Dr Rais Yatim, Malaysia's Information, Communication, and Culture Minister, stated that Malaysia enacted the Personal Data Protection Act of 2010 "not only because of rapid commercial development involving violations of personal data such as credit status of individuals, but also invasion through the means of communication tools being detected and questioned." Datuk Seri Dr Rais Yatim, *Protecting Your Personal Data*, STAR (May 24, 2013, 10:24:27 PM MYT), http://www.thestar.com.my/News/Nation/2012/02/12/Protecting-your-personal-data/.

[164] *See supra* notes 114–18 and accompanying text.

Country	Regulation	Rationale Cited
Russia	Federal Law No. 242 prohibits the storing of Russians' personal data outside of the Russian Federation.	Users' privacy and security, foreign surveillance,[165] national security
	Federal Law No. 97 requires individuals and legal entities who are information organizers on the Internet to store all data for at least six months in Russian territory.	Users' privacy and security, foreign surveillance, national security
	The Ministry of Communications drafted an order requiring telecommunications and Internet providers to install equipment allowing data collection and retention on their servers for at least twelve hours.	National security, domestic law enforcement
South Korea	The Personal Information Protection Act requires information processors to inform and obtain consent from data subjects for transferring personal information to third party overseas.	Users' privacy and security
	The Land Survey, Waterway Survey and Cadastral Records Act of 2009—replacing the Land Survey Act of 1961—prohibits basic land survey and maps information from being transferred outside the South Korea without authorization of the Minister of Land, Transport and Maritime Affairs.	National security

[165] *See supra* notes 122–25 and accompanying text.

Country	Regulation	Rationale Cited
Vietnam	The Decree on Management, Provision, and Use of Internet Services and Information Content Online (Decree 72) requires Internet service providers to place at least a local server inside Vietnamese territory for law enforcement purposes.	Domestic law enforcement,[166] users' privacy and security[167]

II. ANALYSIS

The country studies above reveal the pervasive efforts across the world to erect barriers to the global Internet. But can these measures that break the World Wide Web be justified by important domestic policy rationales? Governments offer a variety of arguments for data localization, from avoiding foreign surveillance to promoting users' security and privacy to bolstering domestic law enforcement and securing domestic economic development. We consider below these four justifications, as well as the costs they will impose on the economic development and political and social freedom across the world.

We leave for a later study a crucial additional concern—the fundamental tension between data localization and trade liberalization obligations.[168] Data

---

166 Nguyễn Dũng [Dung Nguyen], *Bộ Trưởng Nguyễn Bắc Son: Nghị định 72 Bảo Vệ Lợi Ích Người Dùng Internet* [*Minister Nguyễn Bắc Son: Decree 72 Protects the Interests of Internet Users*], INFONET.VN (Aug. 31, 2013, 06:30), http://infonet.vn/bo-truong-nguyen-bac-son-nghi-dinh-72-bao-ve-loi-ich-nguoi-dung-internet-post96412.info (Viet.) (Interview with Minister of Information and Communications Nguyen Bac Son: "Nghị định 72 là cơ sở pháp lý quan trọng để Bộ TT&TT và các cơ quan chức năng xử lý các trang mạng tự ý khai thác, sử dụng thông tin từ các báo mà không được phép, tự ý biên tập làm thay đổi nội dung tác phẩm báo chí. Đây là các hành vi vi phạm luật về bản quyền, gây tổn hại về uy tín, hiệu quả hoạt động của các cơ quan báo chí." ["Decree 72 is an important legal instrument for the Ministry of Information and Communications and government authorities to manage websites that exploit and use news and information published by news agencies without permission and those that independently edit and alter the content of news articles. These are activities that infringe copyrights law, damage reputation, and undermine the operation of news agencies."] (translation by author)).

167 *Id.* ("Trước khi có Nghị định 72, các cơ quan chức năng của Việt Nam cũng đã truy tìm ra được những thủ phạm đã mạo danh gây tổn hại về uy tín, tài sản của người khác để xử lý theo pháp luật. Nghị định 72 chính là cơ sở pháp lý bảo đảm cho việc truy tìm và xử lý các hành vi sai phạm trên được thực hiện nhanh chóng, thuận lợi và hiệu quả hơn." ["Before the enactment of Decree 72, Vietnamese authorities already have the legal authority to prosecute offenders who, through impersonation or identity theft, harm others' reputation and finance. Decree 72 is the legal instrument to guarantee that wrongdoings can be prosecuted more efficiently."] (translation by author)).

168 For important prior work on related issues, see GOOGLE, INC., ENABLING TRADE IN THE ERA OF INFORMATION TECHNOLOGIES: BREAKING DOWN BARRIERS TO THE FREE FLOW OF INFORMATION (2009); NAT'L FOREIGN TRADE COUNCIL, PROMOTING CROSS-BORDER DATA FLOWS: PRIORITIES FOR THE BUSINESS COMMUNITY (2013), *available at* http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlows

localization makes impossible the forms of global business that have appeared over the last two decades, allowing the provision of information services across borders. Moreover, protectionist policies barring access to foreign services only invite reciprocal protectionism from one's trading partners, harming consumers and businesses alike in the process by denying them access to the world's leading services.

A. Foreign Surveillance

Beginning on June 5, 2013, the British newspaper *The Guardian* shocked the world with revelations that the U.S. National Security Agency (NSA) had been secretly intercepting personal data of individuals and dignitaries domestically and abroad.[169] Through internal records released by Edward Snowden, a technical specialist working for the NSA, the NSA was accused of monitoring more than thirty-five world leaders[170] and intercepting communications from more than 50,000 computer systems worldwide.[171] Anger at disclosures of U.S. surveillance abroad has led some countries to respond by attempting to keep data from leaving their shores, lest it fall into U.S. or other foreign governmental hands. For example, India's former Deputy National Security Advisor, Nehchal Sandhu, reportedly sought ways to route domestic Internet traffic via servers within the country, arguing that "[s]uch an arrangement would limit the capacity of foreign elements to scrutinize intra-India traffic."[172] The BRICS nations (Brazil, Russia, India, China, and South Africa) are seeking to establish an international network of cables that would create "a network free of US eavesdropping."[173] But does data localization in

NFTC.pdf; Joshua Meltzer, *Supporting the Internet as a Platform for International Trade Opportunities for Small and Medium-Sized Enterprises and Developing Countries* (Brookings Inst., Working Paper No. 69, 2014), *available at* http://www.brookings.edu/~/media/Research/Files/Papers/2014/02/internet%20international%20trade%20meltzer/02%20international%20trade%20version%202.pdf.

169 Greenwald, *supra* note 2; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013, 15.23 EDT), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. For a review of the major revelations, see Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

170 James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, GUARDIAN (Oct. 24, 2013, 02.50 EDT), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

171 Floor Boon, Steven Derix & Huib Modderkolk, *NSA Infected 50,000 Computer Networks with Malicious Software*, NRC.NL (NETH.) (Nov. 23, 2013, 02:40), http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/.

172 *See* Thomas, *supra* note 3.

173 Paul Joseph Watson, *BRICS Countries Build New Internet to Avoid NSA Spying*, INFOWARS.COM (Oct. 24, 2013), http://www.infowars.com/brics-countries-build-new-internet-to-avoid-nsa-spying/.

fact stave off foreign surveillance? There are significant reasons to be skeptical of this claim.

First, the United States, like many countries, concentrates much of its surveillance efforts abroad. Indeed, the Foreign Intelligence Surveillance Act is focused on gathering information overseas, limiting data gathering largely only when it implicates U.S. persons.[174] The recent NSA surveillance disclosures have revealed extensive foreign operations.[175] Indeed, constraints on domestic operations may well have spurred the NSA to expand operations abroad. As the *Washington Post* reports, "Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight."[176] Deterred by a 2011 ruling by the Foreign Intelligence Surveillance Court barring certain broad domestic surveillance of Internet and telephone traffic,[177] the NSA may have increasingly turned its attention overseas.

Second, the use of malware eliminates even the need to have operations on the ground in the countries in which surveillance occurs. The Dutch newspaper *NRC Handelsblad* reports that the NSA has infiltrated every corner of the world through a network of malicious malware.[178] A German computer expert noted that "data was intercepted here [by the NSA] on a large scale."[179] The *NRC Handelsblad* suggests that the NSA has even scaled the Great Firewall of China,[180] demonstrating that efforts to keep information inside a heavily secured and monitored ironclad firewall do not necessarily mean that it cannot be accessed by those on the other side of the earth. This is a commonplace phenomenon on the Internet, of course. The recent enormous security breach of millions of Target customers in the United States likely sent credit card data of

---

174 *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885c (2012).

175 Andrea Peterson, *The NSA's Global Spying Operation in One Map*, WASH. POST, Sept. 17, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/17/the-nsas-global-spying-operation-in-one-map/.

176 Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, 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.

177 *FISA Court Ruling on Illegal NSA E-mail Collection Program*, WASH. POST, http://apps.washingtonpost.com/g/page/national/fisa-court-documents-on-illegal-nsa-e-mail-collection-program/409/ (last visited Feb. 6, 2015).

178 Boon, Derix & Modderkolk, *supra* note 171.

179 Gabriel Borrud, *Germany Looks to Erect IT Barrier*, DEUTSCHE WELLE (Apr. 11, 2013), http://www.dw.de/germany-looks-to-erect-it-barrier/a-17203480.

180 Boon, Derix & Modderkolk, *supra* note 171.

Americans to servers in Russia, perhaps through the installation of malware on point-of-sale devices in stores.[181]

Third, while governments denounce foreign surveillance on behalf of their citizens, governments routinely share clandestinely intercepted information with each other.[182] *The Guardian* reports that Australia's intelligence agency collects and shares bulk data of Australian nationals with its partners—the United States, Britain, Canada, and New Zealand (collectively known as the "5-Eyes").[183] Even while the German government has been a forceful critic of NSA surveillance, the German intelligence service has been described as a "prolific partner" of the NSA.[184] *Der Spiegel* reports that the German foreign intelligence agency *Bundesnachrichtendienst* (BND) has been collaborating with the NSA, passing about 500 million pieces of metadata in the month of December 2012 alone.[185] The NSA has collaborated with the effort led by the British intelligence agency Government Communications Headquarters (GCHQ) to hack into Yahoo!'s webchat service to access unencrypted webcam images of millions of users.[186] A German computer expert observes, "We know now that data was intercepted here on a large scale. So limiting traffic to Germany and Europe doesn't look as promising as the government and [Deutsche Telekom] would like you to believe."[187]

Fourth, far from making surveillance more difficult for a foreign government, localization requirements might in fact make it easier. By compelling companies to use local services rather than global ones, there is a greater likelihood of choosing companies with weak security measures. By

---

[181] *See* Brian Krebs, *Hacker Ring Stole 160 Million Credit Cards*, KREBS ON SECURITY (July 13, 2013, 3:39 PM ET), http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/ (describing Russians indicted in the United States for earlier identity theft of Americans).

[182] *See infra* note 276 and accompanying text for a discussion of the Mutual Legal Assistance Treaty information sharing procedures.

[183] Ewan MacAskill, James Ball & Katharine Murphy, *Revealed: Australian Spy Agency Offered to Share Data About Ordinary Citizens*, GUARDIAN (Dec. 1, 2013, 19:20 EST), http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens.

[184] *'Prolific Partner': German Intelligence Used NSA Spy Program*, SPIEGEL ONLINE INT'L, (July 20, 2013, 6:02 PM), http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html.

[185] Hubert Gude, Laura Poitras & Marcel Rosenbach, *Mass Data: Transfers from Germany Aid US Surveillance*, SPIEGEL ONLINE INT'L (Aug. 5, 2013, 12:32 PM), http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

[186] Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, GUARDIAN (Feb. 28, 2014, 05.31 EST), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

[187] Borrud, *supra* note 179 (internal quotation marks omitted).

their very nature, the global services are subject to intense worldwide competition, while local services—protected by the data localization requirements—might have less need to offer stronger security to attract customers, and fewer resources to do so, than companies with a global scale. Weaker security makes such systems easier targets for foreign surveillance. This is what we call the "Protected Local Provider" problem.

Fifth, data localization might actually facilitate foreign surveillance. Centralizing information about users in a locality might actually ease the logistical burdens of foreign intelligence agencies, which can now concentrate their surveillance of a particular nation's citizens more easily. We call this the "Jackpot" problem.

Finally, we note that the United States is hardly alone in laws empowering authorities to order corporations to share data of private persons. A recent study shows that such powers are widespread.[188] Indeed, some other states permit access to data without requiring a court order.[189] That is, one state could require a multinational Internet service provider to store all its data on local servers, but that fact does not bar another state from requiring the same multinational provider to turn over data on those servers.

One data localization measure—South Korea's requirement that mapping data be stored in the country—seems especially difficult to defend. After all, under the rules, one can access South Korean maps from abroad freely, as long

---

[188] *See* WINSTON MAXWELL & CHRISTOPHER WOLF, HOGAN LOVELLS, A GLOBAL REALITY: GOVERNMENT ACCESS TO DATA IN THE CLOUD 3 (rev. ed. 2012), *available at* http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf [hereinafter HOGAN LOVELLS WHITE PAPER].

[189] In France, the government can obtain data directly from ISPs without a court order. Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [Law 2006-64 of January 23, 2006, Anti-Terror Act], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 24, 2006, p. 19 (Fr.), *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053177. Under Germany's Telecommunications Act, the government has a right to request data stored by telecommunications companies to advance certain prosecutorial and protective functions. Telekommunikationsgesetz [TKG] [Telecommunications Act] June 22, 2004, BGBL. I at 1190, § 112 (Ger.), *available at* http://www.gesetze-im-internet.de/tkg_2004/index.html, *translation available at*, http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/telekommunkationsgesetz-en,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf. A member of the Irish Garda Síochána not below the rank of chief superintendent may request a service provider to disclose to that member data retained by the service provider under certain conditions. Communications (Retention of Data) Act (Act No. 3/2011), § 6 (Ir.), *available at* http://www.irishstatutebook.ie/2011/en/act/pub/0003/print.html.

as services are themselves based in South Korea.[190] Thus, if a foreigner wants to access online maps of South Korea, it simply needs to turn to Naver and Daum, services that use servers located in that country.[191] As Yonsei University Business School Professor Ho Geun Lee stated, should North Korea want, it can use Naver and Daum's services to view street maps and photographs of streets.[192]

In sum, as Emma Llansó of the U.S.-based Center for Technology and Democracy warns with respect to Brazil's attempt to block information from leaving that country, data localization "would not necessarily keep Brazilians' data out of the NSA's hands."[193] One security professional observes, "The only way to really make anything that is NSA proof is to not have it connect to the Internet."[194]

B. Privacy and Security

Closely related to the goal of avoiding foreign surveillance through data localization is the goal of protecting the privacy and security of personal information against nongovernmental criminal activities. As the country studies above show, the laws of many countries make it difficult to transfer personal data outside of national borders in the name of privacy and security. While these laws are not explicitly designed to localize data, by creating significant barriers to the export of data, they operate as data localization measures.

---

[190] A user in the United States can access maps of South Korea via either Naver or Daum. *See supra* notes 132–36 and accompanying text.

[191] Additionally, one might note that sensitive locations such as the Blue House (the President's residence) or military compounds can be removed from foreign services, as well as domestic ones, at the request of the South Korean government. Lan Goh, *'Jido, Haeoe Ban Chul Hamyeon Cheobeol' 50nyeon Jeon Gasie Changjog Hyeongje Balmok* [*Punishment Imposed if Map Data is Exported Overseas, "Creative Economy" Impeded by 50-year-old Thorn*], JOONGANG ILBO (S. Kor.) (Aug. 20, 2013), http://article.joins.com/news/article/article.asp?total_id=12380240&cloc=olink|article|default (noting that sensitive information is already excluded after examination by government officials).

[192] Ho Geun Lee, *Jido Deiteo, Ijen Segyewa Gyeongjaeng Haja* [*Map Data, Let's Compete with the World*], DIGITAL TIMES (Sept. 26, 2013), http://www.dt.co.kr/contents.html?article_no=2013092702012351607001 (S. Kor.).

[193] Emma Llansó, *Momentum Builds for Brazil's Internet Rights Law*, CENTER FOR DEMOCRACY & TECH. (Sept. 27, 2013), https://cdt.org/blog/momentum-builds-for-brazil%E2%80%99s-internet-rights-law/.

[194] Jon Swartz, *NSA Surveillance Hurting Tech Firms' Business*, USA TODAY, Feb. 28, 2014, http://www.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/ (internal quotation marks omitted).

The irony is that such efforts are likely to undermine, not strengthen, the privacy and security of the information.[195] First, localized data servers reduce the opportunity to distribute information across multiple servers in different locations. As we have noted above, the information gathered together in one place offers a tempting jackpot, an ideal target for criminals. As some computer experts have noted, "Requirements to localize data . . . only make it impossible for cloud service providers to take advantage of the Internet's distributed infrastructure and use sharding and obfuscation on a global scale."[196] Sharding is the process in which rows of a database table are held separately in servers across the world—making each partition a "shard" that provides enough data for operation but not enough to re-identify an individual.[197] "The correct solution," Pranesh Prakash, Policy Director with India's Centre for Internet and Society suggests, "would be to encourage the creation and use of de-centralised and end-to-end encrypted services that do not store all your data in one place."[198]

Second, as we noted above, the Protected Local Provider offering storage and processing services may be more likely to have weak security infrastructure than companies that continuously improve their security to respond to the ever-growing sophistication of cyberthieves. As a recent cover feature of the *IEEE Computer Society* magazine observes, "The most common threats to data in the cloud involve breaches by hackers against inadequately protected systems, user carelessness or lack of caution, and engineering errors."[199] Information technology associations from Europe, Japan, and the United States have echoed this observation, arguing that "security is a function of how a product is made, used, and maintained, not by whom or where it is made."[200] When Australia was contemplating a rule requiring health data to

---

195 Daniel Castro, *The False Promise of Data Nationalism*, INFO. TECH. & INNOVATION FOUND. 1 (Dec. 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf ("The notion that data must be stored domestically to ensure that it remains secure and private is false.").

196 Patrick S. Ryan, Sarah Falvey & Ronak Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, COMPUTER, Dec. 2013, at 54, 56.

197 David Geer, *Big Data Security, Privacy Concerns Remain Unanswered*, COMPUTERWORLD (Dec. 5, 2013, 22:43), http://news.idg.no/cw/art.cfm?id=B1920F48-0FD6-A5E7-5685FC364B81ECBB.

198 Rohin Dharmakumar, *India's Internet Privacy Woes*, FORBES INDIA (Aug. 26, 2013), http://forbesindia.com/article/checkin/indias-internet-privacywoes/35971/1#ixzz2r0zriZTF.

199 Ryan, Falvey & Merchant, *supra* note 196, at 56.

200 Statement, Digital Eur., U.S. Info. Tech. Indus. Council (ITI) & Japan Elecs. & Info. Tech. Indus. Assoc. (JEITA), Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity (June 2012), *available at* http://www.jeita.or.jp/english/topics/2012/0622/release_2012_en.pdf. This idea is echoed in submissions from a range of IT consortia.

remain in the country (a rule that was subsequently implemented), Microsoft made a similar argument. Microsoft argued that the rule might undermine the security of Australian health information by limiting consumer choice among potential providers and wrote, "Consumers should have the ability to personally control their [personal electronic health records] by choosing to have their [personal electronic health records] held by an entity not located within Australia's territorial boundaries if they believe that entity can provide to them a service that meets their individual needs."[201]

Indeed, countries pushing for data localization themselves are sometimes hotbeds of cybercrimes. According to experts, "Cyber security is notoriously weak in Indonesia."[202] Indeed, the nation has been called a "hacker's paradise."[203] One 2013 report on Vietnam suggests that "2,045 agency and business websites were hacked this year, but the number of cyber security experts was too small to cope with all of them."[204] Another account suggests that "Brazil is among the main targets of virtual threats such as malware and phishing."[205] For example, in 2011, hackers stole one billion dollars from companies in Brazil, as *Forbes* put it, the "worst prepared nation to adopt cloud technology."[206] At times, a cybertheft can begin with a domestic burglary, as in the case of one recent European episode.[207] Or cyberthefts can

---

[201] MICROSOFT, PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORDS BILL 2011 – EXPOSURE DRAFT (Oct. 28, 2011) (on file with Emory Law Journal); *see also* Richard Chirgwin, *Microsoft to Aussie Gov: Privacy Rules Stifle e-Health*, REGISTER (Nov. 25, 2011, 00:01), http://www.theregister.co.uk/2011/11/25/ms_threatens_au_gov_over_ehealth/. An Australian local healthcare provider worried about an additional problem with the rule: the proliferation of mobile devices among Australians would inevitably result in information being held overseas as the Australians took these devices abroad; the provider observed, "Consumers will access their data via mobile devices overseas and this will result in data, de facto, being accessed and potentially held or cached, outside of Australia." CSC, *supra* note 15; *see also* Taylor, *supra* note 15 (examining CSC's submission to Parliament).

[202] Jonathan Vit, *Hacker's Paradise or Host Nation? Indonesian Officials Weigh Cyber Threat*, JAKARTAGLOBE (Oct. 25, 2013, 6:34 PM), http://www.thejakartaglobe.com/news/hackers-paradise-or-host-nation-indonesian-officials-weigh-cyber-threat/.

[203] *Id.*

[204] *VN at Risk over Lack of Cyber-Security*, VIỆT NAM NEWS (Oct. 30, 2013, 08:42:00), http://vietnamnews.vn/economy/246923/vn-at-risk-over-lack-of-cyber-security.html.

[205] FROST & SULLIVAN, DOING BUSINESS IN BRAZIL: HOW TO REDUCE YOUR RISKS THROUGH IT INFRASTRUCTURE OUTSOURCING 7 (2012), *available at* http://www.alog.com.br/wp-content/uploads/2012/12/Brazilian_IT_Infrastructure.pdf (emphasis omitted).

[206] Ricardo Geromel, *Hackers Stole $1 Billion in Brazil, The Worst Prepared Nation to Adopt Cloud Technology*, FORBES (Mar. 2, 2012, 8:45 AM), http://www.forbes.com/sites/ricardogeromel/2012/03/02/hackers-stole-1billion-in-brazil-the-worst-prepared-nation-to-adopt-cloud-technology/.

[207] *See* Christopher Thompson, Caroline Binham & Jonathan Guthrie, *ENRC Warns Hackers May Have Stolen Sensitive Data*, FIN. TIMES, May 23, 2013, at 16, *available at* http://www.ft.com/cms/s/0/e25863cc-c392-11e2-8c30-00144feab7de.html.

be accomplished with a USB "thumb" drive. In January 2014, information about more than 100 million South Korean credit cards was stolen, likely through an "inside job" by a contractor armed with a USB drive.[208]

Most fundamentally, there is little reason to believe that the personal information of British Columbians is more secure just because it is stored on a government computer in Vancouver than one owned by IBM, a few miles further south.

C. Economic Development

Many governments believe that by forcing companies to localize data within national borders, they will increase investment at home. Thus, data localization measures are often motivated, whether explicitly or not, by desires to promote local economic development. In fact, however, data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances.

In an Information Age, the global flow of data has become the lifeblood of economies across the world. While some in Europe have raised concerns about the transfer of data abroad, the European Commission has recognized "the critical importance of data flows notably for the transatlantic economy."[209] The Commission observes that international data transfers "form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US."[210] Worried about the effect of constraints on data flows on both global information sharing and economic development, the Organisation for Economic Co-operation and Development (OECD) has urged nations to avoid "barriers to the location, access and use of cross-border

---

[208] Choe Sang-Hun, *Theft of Data Fuels Worries in South Korea*, N.Y. TIMES, Jan. 20, 2014, http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html; Joyce Lee, *South Koreans Seethe, Sue as Credit Card Details Swiped*, REUTERS, Jan. 21, 2014, *available at* http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121.

[209] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 3, COM (2013) 847 final (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[210] *Rebuilding Trust in EU-US Data Flows*, *supra* note 54, at 2.

data facilities and functions" when consistent with other fundamental rights, in order to "ensure cost effectiveness and other efficiencies."[211]

The worry about the impact of data localization is widely shared in the business community as well. The value of the Internet to national economies has been widely noted.[212] Regarding Brazil's attempt to require data localization, the Information Technology Industry Council, an industry association representing more than forty major Internet companies, had argued that "in-country data storage requirements would detrimentally impact all economic activity that depends on data flows."[213] The Swedish government agency, the National Board of Trade, recently interviewed fifteen local companies of various sizes across sectors and concluded succinctly that "trade cannot happen without data being moved from one location to another."[214]

Data localization, like most protectionist measures, leads only to small gains for a few local enterprises and workers, while causing significant harms spread across the entire economy. The domestic benefits of data localization go to the few owners and employees of data centers and the few companies servicing these centers locally. Meanwhile, the harms of data localization are widespread, felt by small, medium, and large businesses that are denied access to global services that might improve productivity. In response to Russia's recently passed localization law, the NGO Russian Association for Electronic Communications stressed the potential economic consequences, pointing to the withdrawal of global services and substantial economic losses caused by the passing of similar laws in other countries.[215] For example, besides the loss of international social media platforms, localization would make it impossible for

---

211 ORG. FOR ECO. CO-OPERATION & DEV., OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY-MAKING 7 (2011), http://www.oecd.org/sti/ieconomy/49258588.pdf.

212 For more information on the economic impact of the Internet and related technologies, see studies compiled by VALUE OF THE WEB, http://www.valueoftheweb.com/ (last visited Feb. 6, 2015).

213 Letter from Info. Tech. Indus. Council Brazil, to Members of the Brazilian Nat'l Congress (Oct. 22, 2013), *available at* https://www.huntonprivacyblog.com/files/2013/11/Brazil-Data-Localization-Letter-English-Version-for-distribution.pdf. Internet companies in Brazil have largely supported the *Marco Civil*, with the significant exception of this particular provision. For a list of members, see *Member Companies*, INFO. TECH. INDUS. COUNCIL, http://www.itic.org/about/member-companies.dot (last visited Feb. 6, 2015).

214 KOMMERSKOLLEGIUM [SWED. NAT'L BD. OF TRADE], NO TRANSFER, NO TRADE: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFER FOR COMPANIES BASED IN SWEDEN 23 (2014), *available at* http://www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf.

215 The Russian Association for Electronic Communications stated, "Passing similar laws on the localization of personal data in other countries has led to withdrawal of global services and substantial economic losses." *New Russian Law Bans Citizens' Personal Data Being Held on Foreign Servers*, RT (July 5, 2014, 10:50), http://rt.com/politics/170604-russia-personal-data-servers/ (emphasis omitted) (internal quotation marks omitted).

Russians to order airline tickets or consumer goods through online services. Localization requirements also seriously affect Russian companies like Aeroflot because the airline depends on foreign ticket-booking systems.[216]

Critics worried, at the time, that the Brazilian data localization requirement would "deny[] Brazilian users access to great services that are provided by US and other international companies."[217] Marilia Marciel, a digital policy expert at Fundação Getulio Vargas in Rio de Janeiro, observes, "Even Brazilian companies prefer to host their data outside of Brazil."[218] Data localization affects domestic innovation by denying entrepreneurs the ability to build on top of global services based abroad. Brasscom, the Brazilian Association of Information Technology and Communication Companies, argues that such obligations would "hurt[] the country's ability to create, innovate, create jobs and collect taxes from the proper use of the Internet."[219]

Governments implementing in-country data mandates imagine that the various global services used in their country will now build infrastructure locally. Many services, however, will find it uneconomical and even too risky to establish local servers in certain territories.[220] Data centers are expensive, all the more so if they have the highest levels of security. One study finds Brazil to be the most expensive country in the Western hemisphere in which to build data centers.[221] Building a data center in Brazil costs $60.9 million on average,

---

216 *Upper House Obligates Internet Companies to Retain Information on Russians Only in Russia*, SPUTNIK NEWS (July 9, 2014, 16:58), http://sputniknews.com/russia/20140709/190859013/Russian-Parliament-Passes-Law-Obliging-Russians-to-Store.html.

217 Joe Leahy, *Brazilian Move Sparks Furore Over Internet Privacy Bid*; *User Data Storage*, FIN. TIMES, Nov. 11, 2013, at 5, *available at* http://www.ft.com/intl/cms/s/0/5cd5b638-487a-11e3-8237-00144feabdc0.html.

218 Esteban Israel & Alonso Soto, *Brazil's Anti-Spying Internet Push Could Backfire, Industry Says*, REUTERS, Oct. 2, 2013, *available at* http://www.reuters.com/article/2013/10/02/us-brazil-internet-idUSBRE9910F120131002 (internal quotation marks omitted).

219 Angelica Mari, *New Data Storage Demands May Put Companies Off Brazil*, ZDNET (Nov. 4, 2013, 17:18 PST), http://www.zdnet.com/new-data-storage-demands-may-put-companies-off-brazil-7000022790/ (internal quotations marks omitted).

220 *See* CUSHMAN & WAKEFIELD, DATA CENTRE RISK INDEX (2013), http://www.cushmanwakefield.com/~/media/global-reports/data-centre-risk-index-2013.pdf.

221 FROST & SULLIVAN, *supra* note 205, at 10; *see also* Israel & Soto, *supra* note 218. Brazil has attempted to address the cost barrier for building local data centers through tax incentives, as part of a broadband infrastructure program, the *Regime Especial de Tributação do Programa Nacional de Banda Larga* (Special Taxation Regime for the Broadband National Program). *See* Decreto No. 7.921, de 18 de Fevereiro de 2013, DIÁRIO OFICIAL DA UNIÃO [D.O.U.], de 18.02.2013 (Braz.), *available at* http://www.jusbrasil.com.br/diarios/50903713/dou-secao-1-18-02-2013-pg-2; *Brazil Signs Tax Relief Measure for Telecom Network Construction*, RCR WIRELESS NEWS (Feb. 19, 2013), http://www.rcrwireless.com/americas/20130219/spectrum/brazils-government-signs-decree-relieve-tax-construction-new-telecom-networks/.

while building one in Chile and the United States costs $51.2 million and $43 million, respectively.[222] Operating such a data center remains expensive because of enormous energy and other expenses—averaging $950,000 in Brazil, $710,000 in Chile, and $510,000 in the United States each month.[223] This cost discrepancy is mostly due to high electricity costs and heavy import taxes on the equipment needed for the center.[224] Data centers employ few workers, with energy making up three-quarters of the costs of operations.[225] According to the 2013 Data Centre Risk Index—a study of thirty countries on the risks affecting successful data center operations—Australia, Russia, China, Indonesia, India, and Brazil are among the riskiest countries for running data centers.[226]

Not only are there significant economic costs to data localization, the potential gains are more limited than governments imagine. Data server farms are hardly significant generators of employment, populated instead by thousands of computers and few human beings. The significant initial outlay they require is largely in capital goods, the bulk of which is often imported into a country. The diesel generators, cooling systems, servers, and power supply devices tend to be imported from global suppliers.[227] Ironically, it is often *American* suppliers of servers and other hardware that stand to be the beneficiaries of data localization mandates.[228] One study notes, "Brazilian suppliers of components did not benefit from this [data localization requirement], since the imported products dominate the market."[229] By increasing capital purchases from abroad, data localization requirements can in fact increase merchandise trade deficits. Furthermore, large data farms are

---

222 Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, WALL ST. J. (Nov. 13, 2013, 6:45 PM ET), http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688 (according to a government-commissioned study seen by *The Wall Street Journal*).

223 *Id.*

224 *See* FROST & SULLIVAN, *supra* note 205, at 10; Israel & Soto, *supra* note 218.

225 *See* RACHEL A. DINES, FORRESTER RESEARCH, INC., BUILD OR BUY? THE ECONOMICS OF DATA CENTER FACILITIES (2011), *available at* https://www.forrester.com/Build+Or+Buy+The+Economics+Of+Data+Center+Facilities/-/E-WEB7855.

226 CUSHMAN & WAKEFIELD, *supra* note 220, at 7.

227 FROST & SULLIVAN, *supra* note 205, at 10.

228 Press Release, Gartner, Gartner Says Worldwide Server Shipments Market Grew 1.3 Percent in the Second Quarter of 2014 While Revenue Increased 2.8 Percent (Aug. 27, 2014), *available at* http://www.gartner.com/newsroom/id/2833020 (noting that US multinational HP, IBM, Dell, Oracle, and Cisco together make up about 76.4 percent of the server market share during the second quarter of 2014).

229 *Brazil Data Center Power Supplies Market Size Report by Frost & Sullivan*, INFOTECH LEAD (Dec. 12, 2013), http://infotechlead.com/2013/12/12/brazil-data-center-power-supplies-market-size-report-frost-sullivan/.

enormous consumers of energy,[230] and thus often further burden overtaxed energy grids. They thereby harm other industries that must now compete for this energy, paying higher prices while potentially suffering limitations in supply of already scarce power.

Cost, as well as access to the latest innovations, drives many e-commerce enterprises in Indonesia to use foreign data centers. Daniel Tumiwa, head of the Indonesian E-Commerce Association (IdEA), states that "[t]he cost can double easily in Indonesia."[231] Indonesia's Internet start-ups have accordingly often turned to foreign countries such as Australia, Singapore, or the United States to host their services. One report suggests that "many of the 'tools' that start-up online media have relied on elsewhere are not fully available yet in Indonesia."[232] The same report also suggests that a weak local hosting infrastructure in Indonesia means that sites hosted locally experience delayed loading time.[233] Similarly, as the Vietnamese government attempts to foster entrepreneurship and innovation,[234] localization requirements effectively bar start-ups from utilizing cheap and powerful platforms abroad and potentially handicap Vietnam from "join[ing] in the technology race."[235]

Governments worried about transferring data abroad at the same time hope, somewhat contradictorily, to bring foreign data within their borders. Many countries seek to become leaders in providing data centers for companies operating across their regions. In 2010, Malaysia announced its Economic Transformation Program[236] to transform Malaysia into a world-class data

---

230 In 2013, datacenters in the United States consumed the equivalent of 34 large (500-megwatt) coal-fired power plants total annual output. NATURAL RES. DEF. COUNCIL, DATA CENTER EFFICIENCY ASSESSMENT 5 (2014), http://www.nrdc.org/energy/files/data-center-efficiency-assessment-IP.pdf.

231 Avi Tejo Bhaskoro, *Indonesia Ministry Still Insists on Local Data Centers for Online Companies*, DAILYSOCIAL (May 8, 2013, 16:28:27), http://en.dailysocial.net/post/indonesian-ministry-still-insists-on-local-data-centers-for-online-companies (internal quotation marks omitted).

232 Ross Settles, *Indonesia: A Hotbed of Innovative Online Publishing Start-ups*, CLICKZ (Mar. 30, 2011), http://www.clickz.com/clickz/column/2281593/indonesia-a-hotbed-of-innovative-online-publishing-startups.

233 *See id.*

234 On June 4, 2013, the Ministry of Science and Technology launched the Silicon Valley Project to stimulate the growth of technology startups in Vietnam. *See* VIETNAM SILICON VALLEY PROJECT, http://www.siliconvalley.com.vn/ (last visited Feb. 6, 2015).

235 *See* Elisabeth Rosen, *Can Vietnam Create the Next Silicon Valley*, ATLANTIC (Feb. 11, 2014, 5:43 PM ET), http://www.theatlantic.com/international/archive/2014/02/can-vietnam-create-the-next-silicon-valley/283760/.

236 *Overview of ETP*, ECON. TRANSFORMATION PROGRAMME, http://etp.pemandu.gov.my/About_ETP-@-Overview_of_ETP.aspx (last visited Feb. 6, 2015).

center hub for the Asia-Pacific region.[237] Brazil hopes to accomplish the same for Latin America, while France seeks to stimulate its economy via a "Made in France" digital industry.[238] Instead of spurring local investment, data localization can lead to the loss of investment. First, there's the retaliation effect. Would countries send data to Brazil if Brazil declares that data is unsafe if sent abroad? Brasscom notes that the Brazilian Internet industry's growth would be hampered if other countries engage in similar reactive policies, which "can stimulate the migration of datacenters based here, or at least part of them, to other countries."[239] Some in the European Union sympathize with this concern. European Commissioner for the Digital Agenda, Neelie Kroes, has expressed similar doubts, worrying about the results for European global competitiveness if each country has its own separate Internet.[240] Then there's the avoidance effect. Rio de Janeiro State University Law Professor Ronaldo Lemos, who helped write the original *Marco Civil* and is currently Director of the Rio Institute for Technology and Society, warns that the localization provision would have caused foreign companies to avoid the country altogether: "It could end up having the opposite effect to what is intended, and scare away companies that want to do business in Brazil."[241] Indeed, such burdensome local laws often lead companies to launch overseas, in order to try to avoid these rules entirely. Foreign companies, too, might well steer clear of the country in order to avoid entanglement with cumbersome rules. For example, Yahoo!, while very popular in Vietnam, places its servers for the

---

[237] *EPP 3: Positioning Malaysia as a World-class Data Centre Hub*, ECON. TRANSFORMATION PROGRAMME, http://etp.pemandu.gov.my/Business_Services-@-Business_Services_-_EPP_3-;_Positioning_Malaysia_As_A_World-class_Data_Centre_Hub.aspx (last visited Feb. 6, 2015); *see also* Edwin Yapp, *Malaysia's Data Center Ambition Faces Challenges*, ZDNET (Apr. 28, 2011, 10:40 GMT), http://www.zdnet.com/malaysias-data-center-ambition-faces-challenges-2062208606/ ("Malaysia has the geographical stability to meet this [growing cloud computing] need."); Edwin Yapp, *Malaysia Must Fulfil Promises to Boost ICT*, ZDNET (Oct. 18, 2010, 10:20 GMT), http://www.zdnet.com/malaysia-must-fulfil-promises-to-boost-ict-2062203784/.

[238] *See* NEW FACE OF INDUSTRY, *supra* note 63, at 1; Press Release, Invest in Fr. Agency, The Growing Market for Cloud Computing in France (Jan. 2012), *available at* http://www.invest-in-france.org/Medias/Publications/1588/cloud-computing-in-France-January-2012.pdf.

[239] Mari, *supra* note 219 (internal quotation marks omitted).

[240] *See* Chiponda Chimbelu, *No Welcome for Deutsche Telekom National Internet Plans from EU Commission*, DEUTSCHE WELLE (Nov. 11, 2013), http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111.

[241] Israel & Soto, *supra* note 218 (internal quotation marks omitted).

country in Singapore.[242] In these ways we see that data localization mandates can backfire entirely, leading to avoidance instead of investment.

Data localization requirements place burdens on domestic enterprises not faced by those operating in more liberal jurisdictions. Countries that require data to be cordoned off complicate matters for their own enterprises, which must turn to domestic services if they are to comply with the law. Such companies must also develop mechanisms to segregate the data they hold by the nationality of the data subject. The limitations may impede development of new, global services. Critics argue that South Korea's ban on the export of mapping data, for example, impedes the development of next-generation services in Korea: Technology services, such as Google Glass, driverless cars, and information programs for visually-impaired users, are unlikely to develop and grow in Korea. Laws made in the 1960s are preventing many venture enterprises from advancing to foreign markets via location/navigation services.[243]

The harms of data localization for local businesses are not restricted to Internet enterprises or to consumers denied access to global services. As it turns out, most of the economic benefits from Internet technologies accrue to traditional businesses. A McKinsey study estimates that about seventy-five percent of the value added created by the Internet and data flow is in traditional industries, in part through increases in productivity.[244] The potential economic impact across the major sectors—healthcare, manufacturing, electricity, urban infra-structure, security, agriculture, retail, etc.—is estimated at $2.7 to $6.2 trillion per year.[245] This is particularly important for emerging economies, in which traditional industries remain predominant. The Internet raises profits as well, due to increased revenues, lower costs of goods sold, and lower administrative costs.[246] With data localization mandates, traditional businesses

---

242 Thu Huong, *VN Digital Content Firms Find Home Disadvantage*, VIỆT NAM NEWS (Sept. 22, 2008), http://vietnamnews.vn/economy/business-beat/180617/vn-digital-content-firms-find-home-disadvantage.html (noting that Yahoo!'s servers serving Vietnam are based in Singapore).

243 *See supra* notes 132–36 and accompanying text.

244 MATTHIEU PÉLISSIÉ DU RAUSAS ET AL., MCKINSEY GLOBAL INST., INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY 22 (2011), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

245 JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 55 (2013), *available at* http://www.mckinsey.com/insights/business_technology/disruptive_technologies.

246 *See* PÉLISSIÉ DU RAUSAS ET AL., *supra* note 244, at 17.

will lose access to the many global services that would store or process information offshore.

Data localization requirements also interfere with the most important trends in computing today. They limit access to the disruptive technologies of the future, such as cloud computing, the "Internet of Things," and data-driven innovations (especially those relying on "big data"). Data localization sacrifices the innovations made possible by building on top of global Internet platforms based on cloud computing. This is particularly important for entrepreneurs operating in emerging economies that might lack the infrastructure already developed elsewhere. And it places great impediments to the development of both the Internet of Things and big data analytics, requiring costly separation of data by political boundaries and often denying the possibility of aggregating data across borders. We discuss the impacts on these trends below.

Cloud Computing. Data localization requirements will often prevent access to global cloud computing services. As we have indicated, while governments assume that global services will simply erect local data server farms, such hopes are likely to prove unwarranted. Thus, local companies will be denied access to the many companies that might help them scale up, or to go global.[247] Many companies around the world are built on top of existing global services. Highly successful companies with Indian origins such as Slideshare and Zoho relied on global services such as Amazon Web Services and Google Apps.[248] A Slideshare employee cites the scalability made possible by the use of Amazon's cloud services, noting, "Sometimes I need 100 servers, sometimes I only need 10."[249] A company like Zoho can use Google Apps, while at the same time competing with Google in higher value-added services.[250]

---

[247] Whether the transfer of information to a cloud service hosted abroad triggers a local privacy law obligation will depend on how the law is interpreted. One report suggests that in Australia, "under the [infrastructure as a service] model . . . the data is not usually '*transferred*' to a third party (ie [sic] the vendor)," and thus does not trigger a data transfer obligation, while the software as a service model (SaaS) might well trigger such an obligation. ALEC CHRISTIE, DLA PIPER CLOUD COMPUTING AND THE NEW AUSTRALIAN PRIVACY LAW (2013), http://www.dlapiper.com/files/Publication/3ecfb49d-c14a-4fab-9645-44d61829f2b1/Presentation/PublicationAttachment/21860e03-439b-43a2-9a44-45746fdd65e1/Cloud%20Computing%20and%20the%20new%20Australian%20Privacy%20Law.pdf.

[248] JONATHAN BOUTELLE, SLIDESHARE, HOW SLIDESHARE USES AMAZON WEB SERVICES (2010), *available at* http://www.slideshare.net/jboutelle/slideshare-aws-talk; Alex Williams, *Zoho Integrates Google Apps and Keeps Step with the Giants*, READWRITE (Dec. 2, 2009), http://readwrite.com/2009/12/01/zoho#awesm=~otx2zoOOYtio6Y.

[249] Boutelle, *supra* note 248, at 4 (internal quotation marks omitted).

[250] Williams, *supra* note 248.

Accessing such global services thus allows a small company to maintain a global presence without having to deploy the vast infrastructure that would be necessary to scale as needed.

The Internet of Things. As the world shifts to Internet-connected devices, data localization will require data flows to be staunched at national borders, requiring expensive and cumbersome national infrastructures for such devices. This erodes the promise of the Internet of Things—where everyday objects and our physical surroundings are Internet-enabled and connected—for both consumers and businesses. Consumer devices include wearable technologies that "measure some sort of detail about you, and log it."[251] Devices such as Sony's Smartband allied with a Lifelog application to track and analyze both physical movements and social interactions[252] or the Fitbit[253] device from an innovative start-up suggest the revolutionary possibilities for both large and small manufacturers. The connected home and wearable computing devices are becoming increasingly important consumer items.[254] A heart monitoring system collects data from patients and physicians around the world and uses the anonymized data to advance cardiac care.[255] Such devices collect data for analysis typically on the company's own or outsourced computer servers, which could be located anywhere across the world. Over this coming decade, the Internet of Things is estimated to generate $14.4 trillion in value that is "up for grabs" for global enterprises.[256] Companies are also adding Internet sensors not just to consumer products but to their own equipment and facilities around the world through RFID tags or through other devices. The oil industry has embraced what has come to be known as the "digital oil field," where real-time

---

[251] Samuel Gibbs & Charles Arthur, *CES 2014: Why Wearable Technology is the New Dress Code*, GUARDIAN (Jan. 7, 2014, 03.29 EST), http://www.theguardian.com/technology/2014/jan/08/wearable-technology-consumer-electronics-show.

[252] *Lifelog*, SONY, http://www.sonymobile.com/global-en/apps-services/lifelog/ (last visited Feb. 6, 2015).

[253] *Who We Are*, FITBIT, http://www.fitbit.com/about (last visited Feb. 6, 2015).

[254] *See* Dan Rowinski, *CES 2014: Connected Homes and Wearables to Take Center Stage*, READWRITE (Jan. 3, 2014), http://readwrite.com/2014/01/03/ces-2014-preview-wearable-technology-4k-tv-connected-home-smartphones-tablets.

[255] *See Why Use It*, ALIVECOR, http://www.alivecor.com/why-use-it (last visited Feb. 6, 2015).

[256] JOSEPH BRADLEY, JOEL BARBIER & DOUG HANDLER, CISCO, EMBRACING THE INTERNET OF EVERYTHING TO CAPTURE YOUR SHARE OF $14.4 TRILLION 3 (2013), http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf. This is the reported "Value at Stake—the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022." *Id.* at 1.

data is collected and analyzed remotely.[257] While data about oil flows would hardly constitute personal information, such data might be controlled under laws protecting sensitive national security information. The Internet of Things shows the risks of data localization for consumers, who may be denied access to many of the best services the world has to offer. It also shows the risk of data localization for companies seeking to better monitor their systems around the world.

Data Driven Innovation (Big Data). Many analysts believe that data-driven innovations will be a key basis of competition, innovation, and productivity in the years to come, though many note the importance of protecting privacy in the process of assembling ever-larger databases.[258] McKinsey even reclassifies data as a new kind of factor of production for the Information Age.[259] Data localization threatens big data in at least two ways. First, by limiting data aggregation by country, it increases costs and adds complexity to the collection and maintenance of data. Second, data localization requirements can reduce the size of potential data sets, eroding the informational value that can be gained by cross-jurisdictional studies. Large-scale, global experiments technically possible through big data analytics, especially on the web, may have to give way to narrower, localized studies. Perhaps anonymization will suffice to comport with data localization laws and thus still permit cross-border data flow, but this will depend on the specifics of the law.

D. Domestic Law Enforcement

Governments have an obligation to protect their citizens, including both preventing harms and punishing those who have committed crimes. Widespread fear of terrorist attacks in particular has led some countries to widen surveillance efforts. The United States expanded its surveillance authority in the wake of the 2001 terrorist attacks with the USA PATRIOT Act[260] and then subsequently with other measures such as the Foreign

---

[257] Jessica Leber, *Big Oil Goes Mining for Big Data*, MIT TECH. REV. (May 8, 2012), http://www.technologyreview.com/news/427876/big-oil-goes-mining-for-big-data/ ("At Chevron, it's the 'i-field.' BP has the 'Field of the Future,' and Royal Dutch Shell likes 'Smart Fields.'").

[258] JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 13 (2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

[259] *Id.* at 3.

[260] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, 115 Stat. 272, 278–96 (codified as amended in scattered sections of the U.S. Code). Sections 202 and 217 of the Act clarify that law

Intelligence Surveillance Act of 1978 Amendments Act of 2008.[261] After the 2008 Mumbai attack in which the terrorists used BlackBerry devices, the Indian government sought access to telecommunications providers' data and asked certain telecommunications providers to locate their servers in India to facilitate access to data by law enforcement.[262] More recently, after the revelations of widespread NSA spying, the Internet Service Providers Association of India, which represents India's domestic Internet Service Providers, asked the government to require foreign internet companies to offer services in that country through local servers, citing concerns for their consumers' privacy.[263] France just recently adopted the law on military programming permitting certain ministries to see "electronic and digital communications" in "real time."[264] While in Vietnam, government officials justify Decree 72 as necessary for law enforcement, including the enforcement of copyright laws regarding news publications and aiding investigation of defamation on social networks.[265]

---

enforcement may seek to intercept electronic communications of "computer trespassers," Section 210 expands the type of information that law enforcement may obtain from Internet Service Providers, Section 211 expands law enforcement's surveillance and investigatory power to cable internet services, and Section 216 simplified the usage authorization of pen registers and trace devices to require only a single court order in order to use these devices on any computer or facility anywhere in the country. For a general discussion of the expanding surveillance, see MARCIA S. SMITH ET AL., CONG. RESEARCH SERV., RL31289, THE INTERNET AND THE USA PATRIOT ACT: POTENTIAL IMPLICATIONS FOR ELECTRONIC PRIVACY, SECURITY, COMMERCE, AND GOVERNMENT (2002), *available at* http://epic.org/privacy/terrorism/usapatriot/RL31289.pdf.

261 Pub. L. No. 110-261, sec. 101(a)(2), § 702(a), 122 Stat. 2436, 2437–38 (2008) (codified at 50 U.S.C. § 1881a (2012)) (empowering the Attorney General and the Director of National Intelligence to authorize surveillance targeting foreign persons and organizations abroad).

262 Praveen Dalal, *Big Brother Must Not Overstep the Limits*, TEHELKA.COM (Mar. 3, 2012), http://www.tehelka.com/big-brother-must-not-overstep-the-limits/ ("Encryption-based service providers such as Research In Motion have been forced to establish servers in India and allow access to messenger services to intelligence agencies in plain, unencrypted form. Nokia has also established a server in India to facilitate law enforcement and intelligence agencies' interception demands."); Noah Shachtman, *How Gadgets Helped Mumbai Attackers*, WIRED (Dec. 1, 2008, 6:39 AM), http://www.wired.com/dangerroom/2008/12/the-gagdets-of/.

263 Vikas SN, *Foreign Internet Companies May Be Asked to Setup Local Servers in India*, MEDIANAMA (June 10, 2013), http://www.medianama.com/2013/06/223-foreign-internet-companies-may-be-asked-to-setup-local-servers-in-india/; Thomas K. Thomas, *Indian Net Firms Want Google, Facebook to Go "Local,"* HINDU BUS. LINE (June 8, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/indian-net-firms-want-google-facebook-to-go-local/article4795367.ece.

264 Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Law No. 2013-1168 of December 18, 2013 on the Military Budget for the Years 2014–2019 and Miscellaneous Provisions for Defense and National Security], art. 20, JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 19, 2013, p. 20570 (Fr.).

265 Nguyen, *supra* note 166.

After a draft of this paper was made available online, we learned that the United States government has, on occasion, exercised its authority to review foreign investments into United States telecommunications infrastructure to require data localization from some of the telecommunications companies.[266] The obligations seem to have arisen as part of the informal "Team Telecom" review of such investments. Team Telecom consists in representatives from the Departments of Justice, Defense, and Homeland Security, as well as the Federal Bureau of Investigation.[267] The inconsistent and varying nature of these obligations—sometimes requiring only prior notice for the use of a foreign service and other times requiring data storage in the United States—suggests that the law enforcement needs are exaggerated. There is no reason to suspect that a criminal is more likely to use one telecommunications provider over another.

Equally important, it seems unlikely that data localization will prove an effective means to ensure that data about their residents is available to law enforcement personnel when they want it. Moreover, other alternatives are reasonably available to assist law enforcement access to data—alternatives that are both less trade restrictive and more speech-friendly than data localization.

Data localization will not necessarily provide law enforcement better access to a criminal's data trail because localization requirements are extremely hard to enforce. They might simply end up driving potential wrongdoers abroad to less compliant and more secretive services. Indeed, the most law-abiding companies will follow costly data localization rules, while others will simply ignore them, comforted by the knowledge that such laws are difficult to enforce. Any success with gaining information from these companies will likely prove temporary, as, over time, potential scofflaws will become aware of the monitoring and turn to services that intentionally skirt the law. The services avoiding the law will likely be foreign ones, lacking any

---

266 *See, e.g.*, Network Security Agreement between U.S. Dep't of Justice, U.S. Dep't of Homeland Sec., U.S. Dep't of Def., and Level 3 Commc'ns, Inc. § 2.5 (2011), *available at* https://info.publicintelligence.net/US-NSAs/US-NSAs-Level3.pdf (requiring that data and communications be stored exclusively in the United States); Network Security Agreement between U.S. Dep't of Justice, U.S. Dep't of Homeland Sec., and TerreStar Corp. § 2.4 (2009), *available at* https://info.publicintelligence.net/US-NSAs/US-NSAs-TerreStar.pdf (requiring that data and communications be made available in the United States); Network Security Agreement between U.S. Dep't of Def., U.S. Dep't of Justice, Fed. Bureau of Investigation, AT&T Corp., British Telecomm. PLC, TNV (Neth.) BV, VLT Co. LLC, and Violet License Co. LLC § 2.5.2 (1999), *available at* https://info.publicintelligence.net/US-NSAs/US-NSAs-ATT.pdf (requiring that prior notice be given to the U.S. Department of Justice before transfer of information abroad).

267 *See* Spencer E. Ante & Ryan Knutson, *U.S. Tightens Grip on Telecom*, WALL ST. J., Aug. 27, 2013, http://online.wsj.com/articles/SB10001424127887324906304579037292831912078.

personnel or assets on the ground against which to enforce any sanction. Thus, understood dynamically, the data localization requirement will only hamper local and law-abiding enterprises, while driving some citizens abroad.

Law enforcement is, without doubt, a laudable goal, so long as the laws themselves do not violate universal human rights. Many governments already have authority under their domestic laws to compel a company operating in their jurisdictions to share data of their nationals held by that company abroad. A recent study of ten countries concluded that the government already had the right to access data held extraterritorially in the cloud in every jurisdiction examined.[268] Although the process varied, "every single country . . . vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders."[269]

Even if companies refuse to comply with such orders, or if the local subsidiary lacks the authority to compel its foreign counterpart to share personal data, governments can resort to information-sharing agreements. For example, the Convention on Cybercrime, which has been ratified by forty-four countries including the United States, France, and Germany,[270] obliges Member States to adopt and enforce laws against cybercrimes and to provide "mutual assistance" to each other in enforcing cyberoffenses.[271] Many states have entered into specific Mutual Legal Assistance Treaties (MLATs) with foreign nations. These treaties establish a process that protects the rights of

---

[268] HOGAN LOVELLS WHITE PAPER, *supra* note 188, at 2–3.

[269] *Id.* at 2–3 (emphasis omitted). The study examines the laws of the following countries: Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, the United Kingdom, and the United States. *Id.* at 3.

[270] Members to the Convention on Cybercrime include the following European countries: Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, the former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom; and the following non-European countries: Australia, Dominican Republic, Japan, Mauritius, Panama, United States. *Status of the Convention on Cybercrime*, COUNCIL OF EUR., http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG (last updated Feb. 7, 2015).

[271] Convention on Cybercrime art. 25(1), Nov. 23, 2001, T.I.A.S. No. 13,174, E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm ("The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.").

individuals yet gives governments access to data held in foreign jurisdictions. Currently, the United States has MLATs in force with fifty-six countries.[272] The United States also entered into a Mutual Legal Assistance Agreement (MLAA) with China and Taiwan.[273] All the countries discussed in the country studies above, with the exception of Indonesia, Kazakhstan, and Vietnam, have MLAT arrangements in force with the United States. Generally, MLATs "specify which types of requested assistance must be provided, and which may be refused."[274] Requests for assistance may be refused typically when the execution of such request would be prejudicial to the state's security or public interest; the request relates to a political offense; there is an absence of reasonable grounds; the request does not conform to the MLAT's provisions; or the request is incompatible with the requested state's law.[275] The explanatory notes to the MLAT between the United States and the European Union observe that a request for data shall only be denied on data protection grounds in "exceptional cases."[276] At the same time, there are procedural requirements to help ensure that the information gathering is supporting a proper governmental investigation. For example, Article 17 of the U.S.–Germany MLAT provides that the government requesting assistance must do

---

[272] 2 BUREAU FOR INT'L NARCOTICS & LAW ENFORCEMENT AFFAIRS, U.S. DEPT. OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT: MONEY LAUNDERING AND FINANCIAL CRIMES 20 (2012), *available at* http://www.state.gov/documents/organization/185866.pdf ("[MLATs] are in force with the following countries: Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, Germany, Greece, Grenada, Hong Kong, Hungary, India, Ireland, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, the Kingdom of the Netherlands (including Aruba, Bonaire, Curacao, Saba, St. Eustatius and St. Maarten), Nigeria, Panama, Philippines, Poland, Romania, Russia, St. Lucia, St. Kitts & Nevis, St. Vincent & the Grenadines, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Trinidad & Tobago, Turkey, Ukraine, United Kingdom (including the Isle of Man, Cayman Islands, Anguilla, British Virgin Islands, Montserrat and Turks and Caicos), Uruguay, and Venezuela.").

[273] *2012 INCSR: Treaties and Agreements*, U.S. DEP'T OF STATE (Mar. 7, 2012), http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm (showing that in addition to MLATs, the United States has a Mutual Legal Assistance Agreement (MLAA) with "China, as well as a MLAA between the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States").

[274] INT'L CHAMBER OF COMMERCE, USING MUTUAL LEGAL ASSISTANCE TREATIES (MLATS) TO IMPROVE CROSS-BORDER LAWFUL INTERCEPT PROCEDURES 3 (2012), http://www.iccindiaonline.org/policy-statement/3.pdf.

[275] THE ALLEGED TRANSNATIONAL CRIMINAL: THE SECOND BIENNIAL INTERNATIONAL CRIMINAL LAW SEMINAR 372–73 (Richard D. Atkins ed., 1995).

[276] Agreement on Mutual Legal Assistance between the European Union and the United States of America, note on art. 9(2)(b), June 25, 2003, T.I.A.S. No. 10-201.1, 2003 O.J. 34; *see also* HOGAN LOVELLS WHITE PAPER, *supra* note 188, at 4.

so in writing and must specify the evidence or information sought, authorities involved, applicable criminal law provisions, etc.[277]

An effective MLAT process gives governments the ability to gather information held on servers across the world. The International Chamber of Commerce has recognized the crucial role of MLATs in facilitating the lawful interception of cross-border data flow and stressed the need to focus on MLATs instead of localization measures.[278] Similarly, the European Commission has recently stressed that the rebuilding of trust in the U.S.–E.U. relationship must focus in part on a commitment to use legal frameworks such as the MLATs.[279] Mutual cooperation arrangements are far more likely to prove effective in the long run to support government information gathering efforts than efforts to confine information within national borders.

E. Freedom

Information control is central to the survival of authoritarian regimes. Such regimes require the suppression of adverse information in order to maintain their semblance of authority. This is because "even authoritarian governments allege a public mandate to govern and assert that the government is acting in the best interests of the people."[280] Information that disturbs the claim of a popular mandate and a beneficent government is thus to be eliminated at all costs. Opposition newspapers or television is routinely targeted, with licenses revoked or printing presses confiscated. The Internet has made this process of information control far more difficult by giving many dissidents the ability to use services based outside the country to share information. The Internet has made it harder, though not impossible, for authoritarian regimes to suppress their citizens from both sharing and learning information.[281] Data localization will erode that liberty-enhancing feature of the Internet.

The end result of data localization is to bring information increasingly under the control of the local authorities, regardless of whether that was originally intended. The dangers inherent in this are plain. Take the following cases. The official motivation for the Iranian Internet, as set forth by Iran's

---

277 Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Ger., art. 17, Oct. 14, 2003, T.I.A.S. No. 09-1018.

278 INT'L CHAMBER OF COMMERCE, *supra* note 274, at 6.

279 *Rebuilding Trust in EU-US Data Flows*, *supra* note 54, at 8.

280 Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 20 (2011).

281 *See, e.g.*, Dong Le, *China Employs Two Million Microblog Monitors State Media Say*, BBC (Oct. 4, 2013, 12:46 ET), http://www.bbc.com/news/world-asia-china-24396957.

head of economic affairs Ali Aghamohammadi, was to create an Internet that is "a genuinely *halal* network, aimed at Muslims on an ethical and moral level," which is also safe from cyberattacks (like Stuxnet) and dangers posed by using foreign networks.[282] However, human rights activists believe that "based on [the country's] track record, obscenity is just a mask to cover the government's real desire: to stifle dissent and prevent international communication."[283] An Iranian journalist agreed, "[t]his is a ploy by the regime," which will "only allow[] [Iranians] to visit permitted websites."[284] More recently, even Iran's Culture Minister Ali Janati acknowledged this underlying motivation: "We cannot restrict the advance of [such technology] under the pretext of protecting Islamic values."[285]

Well aware of this possibility, Internet companies have sought at times to place their servers outside the country in order to avoid the information held therein being used to target dissidents. Consider one example: when it began offering services in Vietnam, Yahoo! made the decision to use servers outside the country, perhaps to avoid becoming complicit in that country's surveillance regime.[286] This provides important context for the new Vietnamese decree mandating local accessibility of data. While the head of the Ministry of Information's Online Information Section defends Decree 72 as "misunderstood" and consistent with "human rights commitments,"[287] the Committee to Protect Journalists worries that this decree will require "both local and foreign companies that provide Internet services . . . to reveal the identities of users who violate numerous vague prohibitions against certain speech in Vietnamese law."[288] As Phil Robertson of Human Rights Watch argues, "This is a law that has been established for selective persecution. This

---

[282] Christopher Rhoads & Farnaz Fassihi, *Iran Vows to Unplug Internet*, WALL ST. J., May 28–29, 2011, at A1, *available at* http://www.wsj.com/articles/SB10001424052748704889404576277391449002016.

[283] Jillian C. York, *Is Iran's Halal Internet Possible?*, ALJAZEERA (Oct. 2, 2012, 08:18), http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html.

[284] *See Government Blocks Google and Gmail, While Promoting National Internet*, REPS. WITHOUT BORDERS (Sept. 24, 2012), http://en.rsf.org/iran-islamic-republic-poised-to-launch-21-09-2012,43431.html.

[285] *Iran's Culture Minister to Loosen Internet Restrictions*, DEUTSCHE WELLE (Mar. 2, 2014), http://www.dw.de/irans-culture-minister-to-loosen-internet-restrictions/a-17468301 (second alteration in original) (internal quotation marks omitted).

[286] *See* Huong, *supra* note 242 (noting that Yahoo!'s servers serving Vietnam are based in Singapore).

[287] *Vietnam Rebuffs Criticism of 'Misunderstood' Web Decree*, REUTERS, Aug. 6, 2013, *available at* http://www.reuters.com/article/2013/08/06/vietnam-internet-idUSL4N0G72IA20130806 (internal quotation marks omitted).

[288] *Decree Targets Online Freedoms in Vietnam*, COMMITTEE TO PROTECT JOURNALISTS (July 22, 2013), http://cpj.org/2013/07/decree-targets-online-freedoms-in-vietnam.php.

is a law that will be used against certain people who have become a thorn in the side of the authorities in Hanoi."[289]

Data localization efforts in liberal societies thus offer cover for more pernicious efforts by authoritarian states. When Brazil's government proposed a data localization mandate, a civil society organization focused on cultural policies compared the measure to the goals of China and Iran:

Translated, this reads as follows: "Understand this: storing data in-country is the Internet dream of China, Iran, and other totalitarian countries, but it is IMPOSSIBLE #MarcoCivil."[290]

Thus, perhaps the most pernicious and long-lasting effect of data localization regulations is the template and precedent they offer to continue and enlarge such controls. When liberal nations decry efforts to control information by authoritarian regimes, the authoritarian states will cite our own efforts to bring data within national control. If liberal states can cite security, privacy, law enforcement, and social economic reasons to justify data controls, so can authoritarian states. Of course, the Snowden revelations of widespread U.S. surveillance will themselves justify surveillance efforts by other states. For example, Russia has begun to use NSA surveillance to justify increasing control over companies such as Facebook and Google.[291] Such rules have led critics to worry about increasing surveillance powers of the Russian state.[292] Critics caution, "In the future, Russia may even succeed in splintering the web,

---

[289] William Gallo & Tra Mi, *New Vietnam Law Bans News Stories from Social Media Sites*, VOICE OF AM. (Aug. 2, 2013, 8:08 AM), http://www.voanews.com/content/new-vietnam-law-bans-news-stories-from-social-media-sites/1722190.html.

[290] *See* Mega Sim, TWITTER (July 20, 2013, 10:13 AM), https://twitter.com/mega_sim/status/358643253043662848. This tweet was last accessed on February 6, 2015.

[291] Kramer, *supra* note 119.

[292] Andrew Soldatov & Irina Borogan, *Russia's Surveillance State*, WORLD POL'Y J., Fall 2013, at 23, *available at* http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

breaking off from the global Internet a Russian intranet that's easier for it to control."[293] Even though officials describe such rules as being antiterrorist, others see a more sinister motive. The editor of Agentura.ru, Andrei Soldatov, believes that Zheleznyak's proposal is motivated by the government's desire to control internal dissent.[294] Ivan Begtin, the director of the group Information Culture, echoes this, arguing that Zheleznyak's surveillance power "will be yet another tool for controlling the Internet."[295] Begtin warns, "In fact, we are moving very fast down the Chinese path."[296]

Finally, creating a poor precedent for more authoritarian countries to emulate is not the only impact on liberty of data localization by liberal states. Even liberal states have used surveillance to undermine the civil rights of their citizens and residents.[297] The proposal for a German "Internetz" has drawn worries that national routing would require deep packet inspection, raising fears of extensive surveillance.[298] The newspaper *Frankfurter Allgemeine* argues that not only would a state-sanctioned network provide "no help against spying," it would lead to "a centralization of surveillance capabilities" for German spy agencies.[299] India's proposed localization measures in combination with the various surveillance systems in play—including Aadhaar, CMS, National Intelligence Grid (Natgrid), and Netra—have raised concerns for human rights, including freedom of expression.[300]

---

293 *Id.* at 24.

294 Alec Luhn, *Moscow's Reaction to Snowden Revelations: Relocate Servers to Russia*, NATION (July 16, 2013), http://www.thenation.com/article/175292/moscows-reaction-snowden-revelations-relocate-servers-russia.

295 Makutina, *supra* note 119.

296 *Id.* (internal quotation marks omitted).

297 *See* Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1059–60 (2002).

298 Richard Adhikari, *Deutsche Telekom Pitches NSA-Free German Internet*, TECH NEWS WORLD (Oct. 26, 2013, 5:00 AM PT), http://www.technewsworld.com/story/79286.html. On deep packet inspection, see Hal Abelson, Ken Ledeen & Chris Lewis, *Just Deliver the Packets*, OFFICE OF THE PRIVACY COMM'R OF CAN., http://www.priv.gc.ca/information/research-recherche/2009/ledeen-lewis_200903_e.asp (last modified Mar. 25, 2009).

299 Alex Evans, *Can Germany Really Keep Bytes Within Its Borders?*, LOCAL (Nov. 29, 2013, 10:10 GMT), http://www.thelocal.de/20131129/german-email-providers-unite-german-internet-against-nsa (internal quotation marks omitted).

300 *India: New Monitoring System Threatens Rights*, HUM. RTS. WATCH (June 7, 2013), http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights ("Indian activists have raised concerns that the CMS will inhibit them from expressing their opinions and sharing information."); Maria Xynou, *India's 'Big Brother': The Central Monitoring System (CMS)*, CTR. INTERNET & SOC'Y (Apr. 8, 2013), http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system ("The overall function of the CMS project and its use of data collected should be thoroughly examined on a legal and

In addition to concerns regarding human rights violations based on surveillance and censorship, data localization measures also interfere with the freedom of expression—particular the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontier[]."[301] Preventing citizens from using foreign political forums because such use might cause personal data to be stored or processed abroad might interfere with an individuals' right to knowledge.[302] Armed with the ability to block information from going out and to filter the information coming in, data location consolidates power in governments by making available an infrastructure for surveillance and censorship.

CONCLUSION

Governments have the right and also the responsibility to insist on the privacy and security of the data of their residents as it crosses borders. They have a variety of tools available to achieve these goals, including contract clauses that commit companies to high security and privacy standards, audits and certifications of foreign suppliers, protections available in the local laws of the foreign suppliers, and adherence to international agreements and standards on such issues, as well as reputational sanctions.[303] Efforts to force data localization distract from efforts to create better protections for individuals across the world. We must insist on data protection without data protectionism. A better, safer Internet for everyone should not require breaking it apart.

---

policy level prior to its operation, as its current vagueness and excessive control over communications can create a potential for unprecedented abuse.").

[301] International Covenant on Civil and Political Rights, art. 19(2), *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force, Mar. 23, 1976); *see also* Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393, 438 (2013).

[302] *See* Molly Beutz Land, *Protecting Rights Online*, 34 YALE J. INT'L L. 1 (2009) (reconceptualizing the access to knowledge movement with the human rights movement in the face of increasing government regulations).

[303] The European Union's Article 29 Working Party opined in 2012 that risk assessment and contractual safeguards (including auditing) were the appropriate means to ensure responsible use of cloud computing services. *Opinion 05/2012 of the Article 29 Working Party on Cloud Computing* (July 1, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp 196_en.pdf. ISO 27001 is a well-accepted international standard for Information Security Management Systems. *ISO/IEC 27001:2005*, WIKIPEDIA, http://en.wikipedia.org/wiki/ISO/IEC_27001:2005 (last modified Feb. 4, 2015).