School of Law

University of California, Davis

400 Mrak Hall Drive

Davis, CA 95616

530.752.0243

http://www.law.ucdavis.edu

UC Davis Legal Studies Research Paper Series

Research Paper No. 378

April 2014

Breaking the Web:

Data Localization vs. the Global Internet

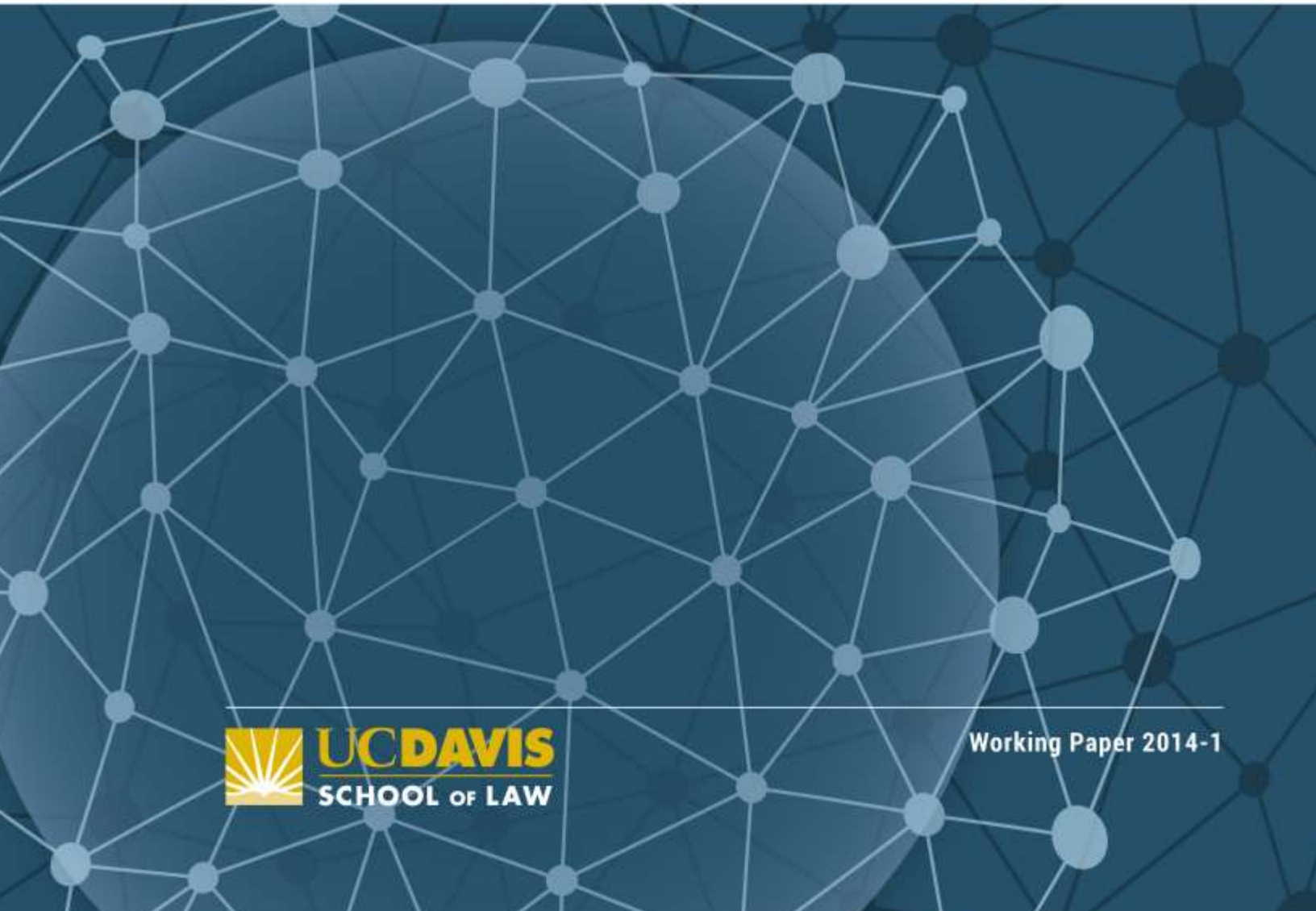
Anupam Chander

Uyen P. Le

CALIFORNIA
INTERNATIONAL
LAW CENTER

Breaking the Web: Data Localization vs. the Global Internet

Anupam Chander
Uyen P. Le



UCDAVIS
SCHOOL OF LAW

Working Paper 2014-1

March 12, 2014

BREAKING THE WEB:
DATA LOCALIZATION VS. THE GLOBAL INTERNET

Anupam Chander*

&

Uyên P. Lê[π]

Abstract

A BRICS Internet, the Euro Cloud, the Iranian 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. South Korea requires mapping data to be stored domestically. Vietnam insists on a local copy of all Vietnamese data. The nations of the world are erecting Schengen zones for data, undermining the possibility of global services. The last century's non-tariff barriers to goods have reappeared as firewalls blocking international services.

Data localization requirements threaten the major new advances in information technology—not only cloud computing, but also the promise of big data and the Internet of Things. Equally important, data localization requirements undermine social, economic and civil rights by eroding the ability of consumers and businesses to benefit from access to both knowledge and international markets and by giving governments greater control over local information. Legitimate global anxieties over surveillance and security are justifying governmental measures that break apart the World Wide Web, without enhancing either privacy or security.

---

* 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, Laura Pedersen, Rachael Smith, and Radhika Tahiliani for very helpful research assistance. The views expressed herein are the authors' alone, as are any errors.

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

TABLE OF CONTENTS

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. 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.[1] 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. Putting data in other nations jeopardizes the security and privacy of such information, the argument goes. 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—from rules preventing information from being sent outside the country, to rules requiring prior consent of the data subject before information is transmitted across national borders, to rules requiring copies of information to be stored domestically, to even a tax on the export of data. We argue here that data localization will backfire, that it in fact undermines privacy and security, while still leaving data vulnerable to foreign surveillance. Even more important, 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

[1] 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 5, 2013), 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. Such intelligence gathering is hardly limited to the United States, of course. David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all (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), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (describing United Kingdom surveillance of global communications).

or planned by many nations to curtail the flow of data outside their borders. Countries around the world are in the process of creating these Checkpoint Charlie's 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 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.[2] 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. Thus, the services built on the Internet, from email to the World Wide Web, pay little heed to national borders. Services such as cloud computing exemplify this, making largely invisible to users the physical locations for the storage and processing of their data. 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.[3] 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 the processing of 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,[4] this paper offers three major advances over earlier work in the area. First, while earlier analyses have referred to a data localization measure

---

[2] TIM BERNERS-LEE, 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").

[3] ANUPAM CHANDER, THE ELECTRONIC SILK ROAD (2013).

[4] Prior studies include U.S. INT'L TRADE COMM'N, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, Pub. 4415, Part 1, Ch. 5 (2013); DANIEL CASTRO, THE INFO. TECH. & INNOVATION FOUND, HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? (2013), *available at* http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry; STEPHEN J. EZELL, ROBERT D. ATKINSON, & MICHELLE A. WEIN, THE 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; ED GRESSER, 21ST-CENTURY TRADE POLICY: THE INTERNET AND THE NEXT GENERATION'S GLOBAL ECONOMY (Jan. 31, 2014), *available at* http://progressive-economy.org/2014/01/31/21st-century-trade-policy-the-internet-and-the-next-generations-global-economy/.

in a country in the most general of terms, our paper 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 paper offers a comprehensive refutation of the various arguments for data localization offered around the world, showing that that data localization measures are in fact likely to undermine security, privacy, economic development, and innovation where adopted.

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—from avoiding foreign surveillance, to enhancing security and privacy, to promoting economic development, and to 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 sixteen states—Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Kazakhstan, Malaysia, Russia, South Korea, Sweden, Taiwan, Thailand, and Vietnam—as well as the European Union. 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. Malaysia, on the other hand, requires consent for international transfer of data, which can prove a significant hurdle. Taiwan permits authorities to restrict transfers if they concern "major national interests." Other regulations focus on selected sectors. Australia prevents health records from being transferred outside the country if they are personally identifiable. In sum, our study reveals the astonishing array of countries that have enacted or are considering data localization.

AUSTRALIA

In 2012, Australia passed the Personally Controlled Electronic Health Records (PCEHR) Act,[5] Section 77 of which prohibits the transfer of health records outside of Australia, with certain exceptions.[6] 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.

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."[7]

BRAZIL

Since 2011, Brazil's Congress has been considering the *Marco Civil da Internet*, which would guarantee Brazilians a significant array of civil rights online.[8] 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.[9] After the NSA surveillance revelations,[10] on November 5, 2013, a new version of the bill was

---

[5] Personally Controlled Electronic Health Records Act, 2012, § 77 (COM.LAW.GOV.AU), http://www.comlaw.gov.au/Details/C2012A00063/Html/Text#_Toc327957207 (last visited March 8, 2014).

[6] *Id.* § 77(1).

[7] *Id.* § 77(2).

[8] Letter from Dean C. Garfield, President and CEO, Info. Tech. Indus. Council, to the Honorable Gleisi Helena Hoffmann, Minister, Casa Civil, Presidency of the Republic, et al. (Aug. 5, 2013), *available at* http://www.itic.org/dotAsset/2a6d7008-9c61-4f7c-917a-5fe4ad493527.pdf [hereinafter Letter from Information Technology Industry Council Brazil]. The *Marco Civil* was inspired by the work of Ronaldo Lemos. Ronaldo Lemos, *Brazilian Internet Needs Civil Regulatory Framework*, UNIVERSO ONLINE (May 22, 2007), http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm.

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

[10] Angelica Mari, *Brazilian Government Tries to Deal with NSA Spying*, ZDNET (July 8, 2013), http://www.zdnet.com/brazilian-government-tries-to-deal-with-nsa-spying-7000017771/; Glenn Greenwald, Robert Kaz & José Casado, *EUA Espionaram Milhões de*

introduced by House of Representatives Framework Rapporteur Alessandro Molon (Workers Party Member from Rio de Janeiro), at the request of President Dilma Rousseff.[11] The new version included an important new power for the executive branch: the ability to require that data about Brazilians be stored in Brazil. Article 12 of the new proposed *Marco Civil* provides:

> 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 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.[12]

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.[13]

CANADA

While Canada's national law, the Personal Information Protection and Electronic Documents Act (PIPEDA),[14] does not prohibit the transfer of personal data outside of Canada, cross-border data flow faces provincial prohibitions. 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—to be stored and accessed only in Canada unless one of a few limited exceptions applies.[15]

E-mails e Ligações de Brasileiros, O GLOBO MUNDO (July 6, 2013) (Braz.), http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2lEHZqYwh.

[11] Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil, 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.

[12] Original text of Article 12 of the *Marco Civil da Internet*: "O Poder Executivo, por meio de Decreto, poderá obrigar os provedores de conexão e de aplicações de Internet previstos no art. 11 que exerçam suas atividades de forma organizada, profissional e com finalidades econômicas a instalarem ou utilizarem estruturas para armazenamento, gerenciamento e disseminação de dados em território nacional, considerando o porte dos provedores, seu faturamento no Brasil e a amplitude da oferta do serviço ao público brasileiro." Projeto de Lei n. 2126 de 2011 [Draft Law No. 2126 of 2011], *translated by* Carolina Rossini, Project Director for the Latin America Resource Center at the Internet Governance and Human Rights Programme at the New America Foundation's OTI, IP-WATCH.ORG (Nov. 14, 2013), *available at* http://www.ip-watch.org/weblog/wp-content/uploads/2013/11/MC_Eng_CR_Nov_13_2013.docx.

[13] *Id.* art. 13.

[14] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

[15] British Columbia Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996 ch. 165 § 30.1 (1996), *available at* http://www.bclaws.ca/Recon/document/ID/freeside/96165_00 [hereinafter British

British Columbia's 1996 Freedom of Information and Protection of Privacy Act states, "A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada[.]"[16] Exceptions to this requirement includes situations in which the data subject "has identified the information and consented . . . to it being stored in or accessed from . . . another jurisdiction . . . ."[17] If an individual uses Gmail (presumably based in the United States), not only would she have to consent to the transfer of information to the United States, every Canadian she talks about in her Gmails would have to consent.[18] In addition to requirements similar to those of British Columbia,[19] Nova Scotia's Personal Information International Disclosure Protection Act also permits storage or access outside of Canada if the "head of a public body" determines that it is necessary for its operation.[20]

CHINA

In 2013, the Chinese government issued the Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems (the Guidelines), which took effect on February 1, 2013.[21] Although the Guidelines are a voluntary technical guidance document,[22] they might serve as a regulatory baseline for Chinese judicial authorities and lawmakers. 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:

Columbia Data Protection Act]. Nova Scotia Personal Information International Disclosure Protection Act, S.N.S. 2006, Ch. 3 § 5 (2006), *available at* http://www.canlii.org/en/ns/laws/stat/sns-2006-c-3/latest/sns-2006-c-3.html [hereinafter Nova Scotia Information Protection Act].

[16] British Columbia Data Protection Act, *supra* note 15, at § 30.1(a)-(c).

[17] *Id.* at § 33.1(1)(i.1).

[18] CHANDER, *supra* note 3, at 6.

[19] Nova Scotia Information Protection Act, *supra* note 15, at § 5(1)(a)-(b).

[20] *Id.* at § 5(2)-(4).

[21] 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. The Provisions provide implementing rules for the Decision on Strengthening Protection of Online Information (the Decision), a national law issued in December 2012. *China Dives into Data Protection Regulation*, TAYLORWESSING.COM, (Apr. 2013), http://www.taylorwessing.com/globaldatahub/article_china_dp.html.

[22] COVINGTON & BURLING LLP, CHINA RELEASES NEW NATIONAL STANDARD FOR PERSONAL INFORMATION COLLECTED OVER INFORMATION SYSTEMS 1 (2013), *available at* 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.

> 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 shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas."[23]

Localization obligations also exist in certain sector-specific operations. In 2011, the People's Bank of China (PBOC) issued a Notice to Urge Banking Institutions to Protect Personal Financial Information.[24] Chinese banks and foreign invested commercial banking institutions are required to observe this Notice when collecting, processing and storing personal financial information (PFI).[25] The Notice "prohibits Banks from storing, processing or analyzing outside China any PFI which has been collected in China, or providing PFI collected in China to an offshore entity. Banks outsourcing their data outside of China need to pay special attention to this requirement, especially as the Notice defines PFI very broadly including personal information of identity, property, account, credit, financial transaction, etc."[26]

The Law of the People's Republic of China on Guarding State Secrets would prevent data from being removed from China if it is deemed to contain a state secret. [27] "State secrets" include "matters that have a vital bearing on state security and national interests."[28]

---

[23] For an overview, see Graham Greenleaf & George Yijun Tian, *China Expands Data Protection through 2013 Guidelines: A "Third Line" for Personal Information Protection*, *with a Translation of the Guidelines*, 122 PRIVACY L. & BUS. INT'L REP. 1, 1 (2013).

[24] *Notice to Urge Banking Financial Institutions to Protect Personal Information*, LAWOFCHINA.COM (May 1, 2011), http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid= [hereinafter *Notice*]; Gigi Cheah, *Protection of Personal Financial Information in China*, NORTON ROSE FULBRIGHT (Oct. 2011), http://www.nortonrosefulbright.com/knowledge/publications/56148/protection-of-personal-financial-information-in-china.

[26] Cheah, *supra* note 24. The United States Federal Reserve has simply asked banks to examine the risks associated with outsourcing, whether within the United States or offshore. Federal Reserve, *Guidance on Managing Outsourcing Risk*, Dec. 5, 2013, http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf.

[27] Tom Antisdel & Tarek Chalayini, *The Challenge of Conducting Data Collections Investigations under Unclear Data Privacy Rules*, CHINA BUS. REV. (Oct. 2011), http://www.alixpartners.com/en/LinkClick.aspx?fileticket=gKMFcT0iTqA%3d&tabid=1092.

[28] The Law of the People's Republic of China on Guarding State Secrets (promulgated by the Standing Comm. of the Nat'l People's Cong.), May 9, 1988, art. 2, *translated in* LAWOFCHINA.COM, *available at*, http://www.lawinfochina.com/display.aspx?lib=law&id=1191&CGid=.

EUROPEAN UNION

The European Union's 1995 Data Protection Directive recognized that the free flow of data across borders was necessary to commerce.[29] At the same time, it sought to ensure that data about Europeans was well protected as it traveled the world. Accordingly, it allowed data to be sent outside the European Union (or the European Free Trade Association states) if it was protected adequately either by local law or by contractual arrangement with the foreign company.[30] To date, the European Commission has found twelve jurisdictions as having adequate protection: Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.[31] Given the amount of information exchange 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.[32] Recently, however, the European Union has been reconsidering the Safe Harbor, alongside a major effort to rewrite European Union privacy law altogether. The EU parliamentarian in charge of steering the European Commission's proposed data protection reform, Jan-Phillip Albrecht, released a report in 2012 recommending that the EU discontinue the Safe Harbor framework after enacting major privacy reforms.[33] After the NSA revelations broke, Vice President Viviane Reding declared, "[t]he Safe Harbour agreement may not be so safe after all."[34] The

---

[29] Council Directive 95/46, art. 56 1995 O.J. (L 281) 23, 11 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. ("Whereas cross-border flows of personal data are necessary to the expansion of international trade….").

[30] 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. *Id.* at art. 25.

[31] *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, European Commission, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited Mar. 8, 2014).

[32] For the Safe Harbor Privacy Principles themselves, see Int'l Trade Admin., *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 FED. REG. 45,666 (July 24, 2000).

[33] *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)*, COM (2012) 0011 – C7-0025, (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.

[34] Christopher Wolf, *EU VP Reding Uses PRISM as Lever to Push Enactment of Regulation and Questions EU-US Safe Harbor*, CHRON. OF DATA PROT. (July 19, 2013), http://www.hldataprotection.com/2013/07/articles/international-eu-privacy/eu-vp-

European Parliament also requested the European Commission to review the Safe Harbor.[35] The Commission then published on November 27, 2013 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.[36]

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).[37] The GDPR allows companies to transfer data outside the European Union if appropriate safeguards (such as binding corporate rules) are in place, 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.[38] The Data Protection Seal must be obtained from a data protection authority. The draft would prohibit the transfer to a country where the law permits the local authorities to access personal data from the European Union.[39]

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

reding-uses-prism-as-lever-to-push-enactment-of-regulation-and-questions-eu-us-safe-harbor/.

[35] Resolution on the U.S. National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy, EUR. PARL. DOC. RC-B7-0336, (July 2, 2013), http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN.

[36] *Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final, http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf [hereinafter *Rebuilding Trust in EU-US Data Flows*]; 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/.

[37] Press Release, European Parliament, *Civil Liberties MEPs Pave the Way for Stronger Data Protection in the EU* (Oct. 21, 2013), http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706 /html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU.

[38] *Transfers by Way of Appropriate Safeguards*, 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) 0011 – C7 0025/2012 – COD (2012) 0011 (Oct. 17, 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.

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

cloud.[40] The government has directly invested in two cloud computing enterprises, Numergy and Cloudwatt, with a one-third ownership stake in each.[41] 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.[42] Whether a subsidy to domestic enterprises is a 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] relevant to locate datacenters and servers in [French] national territory in order to better ensure data security," the Digital Economy Minister Fleur Pellerin explained.[43] The government's ambition to promote a "Made in France" label includes efforts in cloud computing, big data, and connected devices.[44] In its national innovation plan, the government declared its goal to "build a France of digital sovereignty."[45]

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.[46] Proponents of

---

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

[41] David Meyer, *A Guide to the French National Cloud(s)*, GIGAOM (Nov. 18, 2013), http://gigaom.com/2013/11/18/a-guide-to-the-french-national-clouds/ (last visited Feb. 28, 2014).

[42] Minister of Industry Arnaud Montebourg declared: "la surexploitation économique de nos données personnelles par des géants de l'Internet qui sont localisés de l'autre côté de l'Atlantique. . . . L'idée n'est pas d'interdire l'exploitation des données personnelles, mais de faire en sorte qu'elle ait lieu sur le territoire où habitent les personnes dont les données sont exploitées. . . . Il faut mettre en place une stratégie de localisation des data centers [les centres où sont stocké es les données], des emplois rattachés à l'exploitation des données personnelles, sur le territoire européen et particulièrement français[.]" V. Wartner, *Arnaud Montebourg: «Google et Facebook agissent ainsi car il n'y a pas de règles,»* 20 MINUTES.FR (Feb. 28, 2013) (Fr.), http://www.20minutes.fr/politique/1109303-arnaud-montebourg-nous-faisons-tous-jours-lois-citoyens-pourquoi-contre-geants-linternet.

[43] Valéry Marchive, *France Hopes to Turn PRISM Worries into Cloud Opportunities*, VIVE LA TECH (Jun. 21, 2013), http://www.zdnet.com/france-hopes-to-turn-prism-worries-into-cloud-opportunities-7000017089/.

[44] President François Hollande announced a national innovation program on Sep. 12, 2013. MINISTRY OF ECONOMIC REGENERATION, THE NEW FACE OF INDUSTRY IN FRANCE 1 (2013), *available at* http://www.redressement-productif.gouv.fr/files/nouvelle_france_industrielle_english.pdf.

[45] *Id.* at 51.

[46] PIERRE COLLIN & NICHOLAS COLIN, TASK FORCE ON TAX'N DIGITAL ECON., REPORT TO THE MINISTER FOR THE ECONOMY AND FINANCE, THE MINISTER FOR INDUSTRIAL RECOVERY, THE MINSTER 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.

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."[47] The so-called "data tax" would apply to "data derived from the *regular and systematic monitoring of users' activity.*"[48] 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.[49] If France were to declare that data processing in the United States was non-compliant even when conducted under the Safe Harbor,[50] such a tax would effectively become a tax on the export of data. One report notes the possibility of "a global trade war taking place under the guise of taxation."[51]

In March 2012, France adopted Decree No. 2012-436 to amend Section D98-7 of the Code of Electronic Communications relating to lawful interceptions for the protection of public order, national defense, and security.[52] Article 27 of the decree

---

[47] *Id.* at 122.

[48] *Id.* at 123.

[49] "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." *Id.* at 123.

[50] The report accompanying the proposal suggests that compliance might mean going beyond complying with the letter of the law. *Id.* at 124 ("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.").

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

[52] Décret n° 2012-436 du 30 mars 2012 Portant Transposition du Nouveau Cadre Réglementaire Européen des Communications Électroniques [Decree No. 2012-436 of Mar. 30, 2012], Journal Officiel de la République Française [J.O][Official Gazette of France], Mar. 31, 2012, p. 5907, art. 30, *available at* http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025597103&categorieLien=id.

> ("Ces moyens sont mis en place et mis en œuvre dans les conditions suivantes:
>
> - ils sont mis en place sur le territoire national;
>
> - ils sont mis en œuvre sur le territoire national et ne peuvent pas l'être à partir d'un pays étranger;
>
> - les données produites par les systèmes utilisés sont chiffrées par un moyen validé par l'Etat lorsque ces données doivent transiter par voie électronique en dehors du territoire national;
>
> - seuls les agents qualifiés mentionnés au premier alinéa du présent III peuvent utiliser et contrôler les systèmes utilisés pour les interceptions de communications électroniques, accéder aux données produites par ces systèmes et les communiquer aux demandeurs autorisés.").

imposes "territorial" restrictions on Internet providers—requiring that systems for interception of electronic communications be established and implemented in France.[53] Shortly after President François Hollande expressed outrage over U.S. spying, France adopted the Military Programming Law on December 10, 2013, permitting both the security forces and intelligence services from various ministries (defense, interior, economy, and budget)[54] to see "electronic and digital communications" in "real time."[55]

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.[56] They relied on their authority to suspend data transfers if either the Safe Harbor or the Standard Contractual Clauses permitting data transfer

---

[53] *Id.* at art. 27.

[54] LOI n° 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 [Military Programming Law][Law No. 2013-1168 of Dec. 18 2103], Journal Officiel de la République Française [J.O.] [Official Gazette of France], p. 20570 Dec. 19, 2013, p. 20570, art. 20, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id [hereinafter France Military Programming Law 2013] ("les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.").

[55] *Id.* The legislation has drawn critique. Andréa Fradin, *L'article 13 Est-il Plus Dangereux pour Internet que les Lois Existantes?*, SLATE.FR (Dec. 11, 2013), http://www.slate.fr/story/81011/loi-programmation-militaire-danger (Fr.) (critique of the Association of Internet Community Services (ASIC), 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.

[56] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Datenschutzkonferenz: Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten (July 24, 2013) (F.R.G.), http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html?nn=408908. The Conference of Commissioners consists of sixteen state data protection commissioners along with Federal Data Protection Commissioner Peter Schaar. Press Release, Die Landesbeauftragte für Datenschutz und Informationsfreiheit, *Conference of Data Protection Commissioners Says that Intelligence Services Constitute a Mass Threat to Data Traffic Between Germany and Countries Outside Europe* (July 24, 2013), http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.

have a "substantial likelihood" of violation.[57] The Commissioners argued that the violations arose because data transferred by German companies can be accessed by the NSA and various others foreign intelligence services without complying with limitation principles (*viz.*, need, proportionality, and purpose).[58]

While the Commissioners sought to stop data flow outside Europe, some within Germany proposed to limit data flows only to routes within Germany. In October 2013, Deutsche Telekom (which is one-third state-owned[59]) proposed that data between Germans be routed inside German networks.[60] The idea was also supported by then-Interior Minister Hans-Peter Friedrich. Earlier in August, Deutsche Telekom launched "E-mail made in Germany," a service that seeks to route data exclusively through domestic servers.[61] In February 2014, Chancellor

---

[57] 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), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF; 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), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF.

[58] 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 Kreis, maintained that U.S. Safe Harbor self-certifications should not be automatically considered as conclusive proof of adequate protection. "Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können." Beschluss der obersten Aufsichtsbehör den für den Datenschutz im nicht-öffentlichen Bereich, *Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen*, Apr. 28, 2010, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf;jsessionid=34480CBEFF09F90E0916CE90C8B0E224.1_cid354?__blob=publicationFile. *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), *available at* http://idpl.oxfordjournals.org/content/1/3/143.full.pdf+html.

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

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

[61] *Will It Work? German Email Companies Adopt New Encryption to Foil NSA*, REUTERS (Aug. 9, 2013), http://rt.com/news/german-email-encryption-nsa-312/.

Angela Merkel proposed that Europe build out its own Internet infrastructure designed to keep data within Europe. 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."[62] 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.[63]

INDIA

In April 2011, the Indian Ministry of Communications and Technology published privacy rules implementing certain provisions of the Information Technology Act of 2000.[64] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules limit the transfer of "sensitive personal data or information"[65] abroad to two cases—when "necessary" or when the data subject consents to the transfer abroad. Specifically, Rule 7 provides:

> 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

---

[62] *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.

[63] *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.

[64] The Information Technology Act 2000 ("IT Act") focused on computer misuse, but did not cover data security. The IT (Amendment) Act 2008 added two additional sections, Section 43A and Section 72A, to address the loss and protection of personal data.

[65] 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 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."

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3, DEITY.GOV.IN (Apr. 11, 2011), http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

> 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.[66]

Because it is difficult to establish that it is "necessary" to transfer data, this provision would generally 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. Commentators observed that the consent requirements were "far more restrictive" than what is required under United States or European Union laws.[67] European Union laws require consent for data collection and processing generally, not special consent for transfer abroad. Special consent required for exporting data suggests that data that is 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 sent outside the United States.[68] 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.[69] 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.[70] While patching over one problem, the

---

[66] *Id.*

[67] MIRIAM H. WUGMEISTER & CYNTHIA J. RICH, MORRISON & FOERSTER, INDIA'S NEW PRIVACY REGULATIONS 1 (May 4, 2011), *available at* http://www.mofo.com/files/Uploads/Images/110504-Indias-New-Privacy-Regulations.pdf.

[68] 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, Sect. 4, 2013-2014 Regular Sessions NY Senate Bill S2992-2013 (Jan. 28, 2013).

[69] Alston & Bird, *Questions Answered, More Questions Raised: Exploring the Outsourcing Implications of India's Recently Released Privacy Rules*, June 21, 2011, 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.

[70] Linklaters, *India - Welcome Clarification on Sensitive Personal Data Rules,* Sept. 20, 2011, http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-newsletter-

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]." It provides:

> No 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.[71]

Under the statute, "any … material produced by a computer" constitutes "public records."[72] In 2013, the Delhi High Court interpreted this requirement to bar the transfer of government emails outside India. It ordered the government to formulate a policy for official government email that would comply with the Public Records Act.[73] 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.[74] The information technology directorate of the state of Maharashtra has advised government agencies "to host their websites only on servers located within India" and to use "government provided email IDs, from servers within India" for official communication.[75]

September-2011/Pages/India-data-security-laws.aspx#sthash.oGD5gPZG.dpuf; 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, http://pib.nic.in/newsite/erelease.aspx?relid=74990.

[71] Public Records Act, No. 69 of 1993, INDIA CODE (1993), § 4, *available at* http://www.delhi.gov.in/wps/wcm/connect/doit_art/Art+Culture+and+Language/Home/Department+of+Archives/Acts+and+Rules/.

[72] *Id.* § 2(e)(iv).

[73] K.N. Govindacharya v. Union of India and ORS, W.P.(C) 3672/2012, CM Nos.7709/2012, 12197/2012 and 6888/2013, High Court of Delhi (Oct. 30, 2013), http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=211444&yr=2013 (last visited Mar. 1, 2014).

[74] Standing Committee on Information Technology, Cyber Crime, Cyber Security And Right To Privacy Fifty-Second Report 21 (Feb. 2014), https://www.dsci.in/sites/default/files/15_Information_Technology_52.pdf.

[75] Letter from Rajesh Aggarwal, Secretary of Information Technology, Directorate of Information Technology to Maharashtra Gov. Dept. 2 (Sep. 30, 2013), https://www.maharashtra.gov.in/Site/upload/WhatsNew/Advisory%20dated%20300913.pdf.

In February 2014, the National Security Council (NSC) proposed a policy that might require data localization by Indian citizens, and not just government agencies alone. According to an NSC internal note seen by the newspaper *The Hindu*, "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[.]"[76] The NSC proposal would prohibit "[a]s a general principle, mirroring of data in these servers to main servers abroad[.]"[77] 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 (NIXI) to ensure that domestic Internet packets remains mostly in India. 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."[78]

INDONESIA

In 2012, the Indonesian government required service providers providing "public services" to place their data centers within the country. Regulation 82 on the Operation of 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."[79] Although the term "public services" is defined in the Public Service Law of 2009,[80] this provision did not define exactly what kinds of "electronic system operators" were deemed to be in the "public service."[81] A Draft Regulation Concerning

[76] Thomas K. Thomas, *National Security Council Proposes 3-Pronged Plan to Protect Internet Users,* HINDU (Feb. 13, 2014) http://www.thehindubusinessline.com/features/smartbuy/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece (last visited Mar. 1, 2014).

[77] *Id.*

[78] Standing Committee on Information Technology, *supra* note 74, at 61.

[79] 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), *translated in* 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.

[80] Undang-Undang Tentang Pelayanan Publik [Public Service Law], Law No. 25/2009, Jul. 18, 2009 (Government Gazette of the Republic of Indonesia Year 2009 No. 112) *available at* http://www.setneg.go.id//components/com_perundangan/docviewer.php?id=2274&filename=UU%2025%20Tahun%202009.pdf.

[81] *Id.* at art. 5 (Public services are services (a) provided by government agencies, (b) fully or partially funded by state budget, (c) none of the above but whose delivery is part

Registration Procedure of Electronic System Provider clarifies this somewhat, explaining that "public service electronic systems by the private business sector" include "[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; … [is] used to process electronic information …[or] is provided for sending of paid files over the internet, including those that are downloaded via an internet gate or site, e-mail sending or that sending by another application to a device user."[82] On its face, this approach seems so broad that almost all websites and online applications such as newspapers or blogs might be "public services" because they "process electronic information." However, idEA, the Indonesian Association of E-commerce, has criticized this interpretation as inconsistent with regulations on public services.[83]

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.[84] 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," from "Google and Yahoo to hotels, banks, and airlines services."[85] 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.

---

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.).

[82] Rancangan Peraturan Menteri (RPM) tentang Tata Cara Pendaftaran Penyelenggaraan dan Sistem Transaksi Elektronik [Draft Regulation Concerning the Registration Procedure of Electronic System Provider], art. 4 (translation on file with authors).

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

[84] Rancangan Peraturan Menteri (RPM) tentang Pedoman Teknis Pusat Data [Draft Regulation Concerning the Technical Guidelines for Data Centers] (2013), *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* (Jan. 7, 2014), 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 (last visited Feb. 24, 2014).

[85] *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/ (last visited Mar. 1, 2014); Vanesha Manuturi & Basten Gokkon, *Web Giants to Build Data Centers in Indonesia?* JAKARTA GLOBE (Jan. 15, 2014), http://www.thejakartaglobe.com/news/web-giants-to-build-data-centers/ (last visited Feb. 25, 2014).

MALAYSIA

In 2010, Malaysia passed the Personal Data Protection Act (PDPA), which requires data about Malaysians to be stored on local servers.[86] 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.

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 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 which 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.[87] 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.

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 data of Russian clients on servers inside the country, where they would be subject to domestic law enforcement search warrants."[88]

---

[86] Personal Data Protection Act, Law No. 709 of 2010, Official Gazette of Malaysia, June 10, 2010, P.U. (B) 464, *available at* http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf (last visited Mar. 1, 2014).

[87] *Id.* at art. 129(3).

[88] Andrew E. Kramer, *N.S.A. Leakers Revive Push in Russia to Control Net*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?pagewanted=1&_r=2 (last visited Mar. 1, 2014); Maria Makutina, *Lawmakers Seek to Bolster Russia's Internet Sovereignty*, RUSSIA BEYOND THE HEADLINES (June 21, 2013), http://rbth.ru/politics/2013/06/21/lawmakers_seek_to_bolster_russias_internet_sovereignty_27365.html (last visited Mar. 1, 2014).

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 twelve hours.[89] 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), IP addresses and location data—without a court order, for the purposes of national anti-terrorist investigations."[90]

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.[91] Article 17(3) of the Act targets data exports for a special protection regime:

> When the personal information processor provides personal information to a third party overseas, it shall inform … and obtain consent from data subjects.

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:

> The recipient of personal information; the recipient's purpose of use of the personal information; particulars of personal information to be provided; the period when personal information is retained and used by said recipient; and the fact that data subjects are entitled to deny consent; and the disadvantage resulting from the denial of consent.

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.

---

[89] Alexandra Kulikova, *Data Collection and Retention in Russia: Going Beyond the Privacy and Security Debate,* GLOBAL PARTNERS (Jan. 17, 2014), http://www.gp-digital.org/gpd-update/data-collection-and-retention-in-russia/ (last visited Mar. 1, 2014).

[90] *Id.*

[91] Personal Information Protection Act, Law No. 10465, South Korea (promulgated on Mar. 29, 2011), *available at* http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf (last visited Mar. 1, 2014). The Personal Information Protection Act replaces 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.

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.[92] The constraint in this law continues to this day, and has been interpreted recently as outlawing mapping data from being held on computer servers outside the country. 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.[93] 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.

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"),[94] 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."[95] The same decree also requires a range of Internet service providers to maintain within Vietnam a copy of any information they hold in order to facilitate the inspection of information by authorities. Specifically, Decree 72 provides that organizations and enterprises must:

> have at least one server system in Vietnam allowing the inspection, checking, storage, and provision of information at the request of competent authorities . . . .[96]

The Decree applies to general websites, social networks, mobile networks, and game service providers.[97] Unlike many other countries, Vietnam's focus is not in

---

[92] "Without the permission of the Minister of Land, Transport and Maritime Affairs of the basic survey and measurement or for maps and photos shall not be taken out of the country." Land Survey Act [Cheukryangbeop Act], Law no. 938 of Dec. 31, 1961, at 16, paragraph 1 (S. Korea).

[93] Geun Ho Lim, *Searching Directions from HanKyung to Seoul Station…Fly over Buildings? Google Map Cannot Navigate only in Korea*, KOREA ECON. DAILY (Dec. 9, 2013), http://www.hankyung.com/news/app/newsview.php?aid=2013120998951 (last visited Feb. 28, 2014).

[94] Decree on Management, Provision and Use of Internet Services and Online Information, No. 72/2013/ND-CP (July 15, 2013) (Vietnam), http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf [hereinafter Decree 72].

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

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

protecting the privacy of the information but in ensuring that information is available to local authorities that want ready access to it.

A 2013 Circular from the Ministry of Information and Communications provides additional implementing details for Decree 72. The Circular again affirms that a central goal of that decree is to assist local authorities in controlling information. The 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.[98]

The 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.[99] Thus, not only must the data reside in Vietnam, so must a high level executive of the company.

---

[97] *Id.* art. 24(2) (general websites); *id.* art. 25(8) (social networks); *id.* art. 28(2) (mobile networks); *id.* art. 34(2) (game service providers).

[98] 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 of Internet Services and Online Information, Circular No. 08/2013/TT-BTTTT of March 26, 2013, art. 8, Vietnamese Ministry of Information and Communication, *available at http://english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/Attachments/6361/08-2013-TT-BTTTT.doc* (last visited Mar. 1, 2014).

[99] *Id.* art. 3 (conditions of granting a license to establish general information websites and social networks:

1. Management personnel:

OTHERS

Kazakhastan—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.[100] The government took steps to enforce this regulation in late 2010, causing Google to redirect traffic to Google.kz to Google.com.[101] The redirect caused search queries to return results that were not customized for Kazakhstan. The Kazakhstani Association of IT Companies later required that the domestic server requirements apply only to new domains registered after September 7, 2010.[102] This allowed Google (which had registered its name well before this date) to restore the Google.kz functionality, but it means that domestic or foreign companies registering a domain name after this date can 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, 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.[103] In 2012, the Norwegian data authority concluded that cities could not use cloud computing services unless the servers were located domestically, but then lifted the ban on the use of Google Apps a short time later.[104]

> 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 . . . .).

[100] FREEDOM HOUSE, KAZAKHSTAN 6 (2013), *available at* http://www.freedomhouse.org/sites/default/files/resources/FOTN%202013_Kazakhstan.pdf (last visited Mar. 1, 2014).

[101] 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 (last visited Mar. 1, 2014)("The 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.").

[102] *Google.kz вернулся в Казахстан* [*Google.kz Returned to Kazakhstan*], TENGRINEWS.KZ (June 15, 2011), http://tengrinews.kz/internet/190571/ (last visited Mar. 1, 2014).

[103] *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/ (last visited Mar. 1, 2014).

[104] Norwegian Data Inspectorate, Notification of decision – New e-mail solution within Narvik local authority (Narvik commune) – Google Apps, DATATILSYNET.NO (Jan. 16, 2012), http://www.datatilsynet.no/Global/english/2012_narvik_google_eng.pdf

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.[105] 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.[106] The Data *Datainspektionen* did eventually approve the use of Dropbox, a U.S.-based cloud service.[107]

Taiwan—Article 21 of Taiwan's Personal Data Protection Act[108] permits government agencies the authority to restrict international transfers in the industries they regulate, under certain conditions such as when the information

(decision to ban service) (last visited Mar. 1, 2014); *Use of Cloud Computing Services*, DATATILSYNET.NO (Sept. 26, 2012), http://www.datatilsynet.no/English/Publications/cloud-computing/ (reporting on the decision to lift the ban) (last visited Mar. 1, 2014); Loek Essers, *Norway ends nine-month ban on Google Apps*, COMPUTER WORLD (Sept. 26, 2012), http://www.computerworld.com/s/article/9231738/Norway_ends_nine_month_ban_on_Google_Apps_use?taxonomyId=158&pageNumber=2 (last visited Mar. 1, 2014).

[105] Dan Jerker & B. Svantesson, *Data protection in cloud computing – The Swedish perspective*, 28 COMPUTER LAW & SECURITY REV. 476 (2012); Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011, DATAINSPEKTIONEN (May 31, 2013) (Swed.), http://www.datainspektionen.se/Documents/beslut/2013-05-31-salems-kommun.pdf (last visited Mar. 1, 2014); Liam Tung, *Sweden Tells Council to Stop Using Google Apps*, ZDNET (Jun. 14, 2013), 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. Jonas Ryberg, *Storbråk om Google Apps*, COMPUTERSWEDEN (Sept. 17, 2013), http://computersweden.idg.se/2.2683/1.523293/storbrak-om-google-apps.

[106] Google, *Data Processing Amendment to Google Apps Enterprise Agreement*, https://www.google.com/intx/en/enterprise/apps/terms/dpa_terms.html (last visited Mar. 1, 2014). The Model Contract Clauses provide for "prior written consent" before the use of subprocessors by the data importer. Commission Decision of Feb. 7, 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, Doc. C(2010) 593.

[107] Jerker & Svantesson, *supra* note 105.

[108] 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.

involves major national interests, by treaty or agreement, inadequate protection, or when the foreign transfer is utilized to avoid Taiwanese laws.[109]

Thailand—Thailand is considering a comprehensive data protection framework.[110] 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.[111]

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 security and privacy to law enforcement and promoting domestic investment. We consider below these 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.[112] Data

---

[109] Personal Information Protection Act, art. 21 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (listing 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 [] 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."). 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. *Taiwan: Telcos Prohibited from Transferring Customer Data to China*, DATA GUIDANCE (Oct. 12, 2012), http://www.dataguidance.com/news.asp?id=1879 (last visited Mar. 1, 2014).

[110] ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. [Draft Personal Data Protection Act]

[111] Thailand Draft Personal Data Protection Act, art. 27.

[112] For important prior work on related issues, see Joshua Meltzer, *Supporting The Internet As A Platform For International Trade Opportunities For Small And Medium-Sized Enterprises And Developing Countries* (Feb. 2014), at http://www.brookings.edu/~/media/Research/Files/Papers/2014/02/internet%20international%20trade%20meltzer/02%20international%20trade%20version%202.pdf; NATIONAL FOREIGN TRADE COUNCIL, PROMOTING CROSS-BORDER DATA FLOWS: PRIORITIES FOR THE BUSINESS COMMUNITY (2013), http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf;

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.

1. FOREIGN SURVEILLANCE

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 Deputy National Security Advisor Nehchal Sandhu has 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."[113] 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."[114] But does data localization in 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 United States persons.[115] The recent NSA surveillance disclosures have revealed extensive foreign operations.[116] 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."[117] Deterred by a 2011 ruling by the Foreign Intelligence Surveillance Court barring certain broad domestic

---

GOOGLE, INC., ENABLING TRADE IN THE ERA OF INFORMATION TECHNOLOGIES: BREAKING DOWN BARRIERS TO THE FREE FLOW OF INFORMATION (2009).

113 Thomas K. Thomas, *Route Domestic Net Traffic via India Servers, NSA Tells Operators*, HINDU (Aug. 14, 2013), http://www.thehindubusinessline.com/industry-and-economy/info-tech/route-domestic-net-traffic-via-india-servers-nsa-tells-operators/article5022791.ece.

114 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/.

115 Foreign Intelligence Surveillance Act, 50 U.S.C.A. § 1801 (2010).

116 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/.

117 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.

surveillance of Internet and telephone traffic,[118] 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 German newspaper *Handelsblatt* reports that the NSA has infiltrated every corner of the world through a network of malicious malware.[119] A German computer expert points out that "data was intercepted here [by the NSA] on a large scale."[120] The *Handelsblatt* report suggests that the NSA has even scaled the Great Firewall of China, 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 Americans to servers in Russia, perhaps through the installation of malware on point of sale devices in stores.[121]

Third, not only do governments spy overseas, governments routinely share information with each other, even outside the official information sharing treaty procedures.[122] *The Guardian* reports that Australia's intelligence agency collects and share bulk data of Australian nationals with its partners—the United States, Britain, Canada, and New Zealand (collectively known as the 5-Eyes).[123] 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. *Der Spiegel* reports that the German foreign intelligence agency *Bundesnachrichtendienst*

---

118 Memorandum Opin., FISA Ct., Oct. 3, 2011 (redacted and unpublished), *available at* http://apps.washingtonpost.com/g/page/national/fisa-court-documents-on-illegal-nsa-e-mail-collection-program/409/.

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

120 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 ("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.").

121 Brian Krebs, *Hacker Ring Stole 160 Million Credit Cards,* KREBS ON SECURITY (July 13, 2013), 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).

122 *See infra* notes 191- 204 and accompanying text for a discussion of the Mutual Legal Assistance Treaty information sharing procedures.

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

(BND) has been collaborating with the NSA, passing about 500 million pieces of metadata in the month of December 2012 alone.[124] 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.[125] 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."[126]

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 their very nature, the global services are subject to intense worldwide competition, while the local services are protected by the data localization requirements. Weaker security makes such systems easier targets for foreign surveillance. This is what we call the "Protected Local Provider" problem.

Fifth, collecting 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. Call this the "Honeypot" problem.

Finally, we might 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.[127] Indeed, some other states permit access to data without requiring a court order.[128]

---

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

[125] Spencer Ackerman & James Ball, *UK Spy Agency Intercepted Webcam Images of Millions of Yahoo Users*, GUARDIAN (Feb. 24, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

[126] *Germany Looks to Erect IT Barrier*, DEUTSCHE WELLE (Nov. 4, 2013), http://www.dw.de/germany-looks-to-erect-it-barrier/a-17203480 (quoting Dirk Engling of the Chaos Computer Club).

[127] WINSTON MAXWELL & CHRISTOPHER WOLF, HOGAN LOVELLS, A GLOBAL REALITY: GOVERNMENT ACCESS TO DATA IN THE CLOUD (2012), *available at* [hereinafter HOGAN LOVELLS WHITE PAPER].

[128] 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], art.6, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 24, 2016, p. 19 (Fr.), *available at*

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 as services are themselves based in South Korea. 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.[129] As Yonsei University Business School Professor Ho Geun Lee notes, "In reality, if North Korea wants to, it can use Naver and Daum's services to view street maps and photographs of streets."[130]

In sum, as Emma Llansó of the U.S.-based Center for Technology and Democracy warns with respect to Brazilians efforts to block information from leaving that country, data localization "would not necessarily keep Brazilians' data out of the NSA's hands."[131] One security professional observes, "The only way to really make anything that is NSA proof is to not have it connect to the Internet."[132]

---

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] §112, June 22, 2004, BGBL. I (Ger.), *available at* http://www.gesetze-im-internet.de/tkg_2004/index.html, *translated in* DIE BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT http://www.bfdi.bund.de/cae/servlet/contentblob/411286/publicationFile /25386/TelecommunicationsAct-TKG.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 2011, Act No. 3 of 2011, §6 (Ir.), *available at* http://www.irishstatutebook.ie/2011/en/act/pub/0003/print.html.

[129] 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, *Punishment Imposed if Map Data is Exported Overseas, "Creative Economy" Impeded by 50-year-old Thorn*, JOONGANG ILBO (Aug. 20, 2013), http://article.joins.com/news/article/article.asp?total_id=12380240&cloc=olink|article|default (sensitive information is already excluded after examination by government officials).

[130] Ho Geun Lee, Commentary, *Map Data, Let's Compete with the World*, DIGITAL TIMES (Sept. 26, 2013), http://www.dt.co.kr/contents.html?article_no=2013092702012351607001.

[131] Emma Llansó, *Momentum Builds for Brazil's Internet Rights Law*, CTR. DEMOCRACY & TEC. (Sept. 27, 2013), https://www.cdt.org/blogs/emma-llanso/2709momentum-builds-brazil%E2%80%99s-internet-rights-law.

[132] Jon Swartz, *NSA Surveillance Hurting Tech Firms' Business*, USA TODAY (Feb. 28, 2014) (quoting Domingo Guerra), *available at* http://www.usatoday.com/story/tech/2014/02/27/nsa-resistant-products-obama-tech-companies-encryption-overseas/5290553/.

2. *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 non-governmental 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.

The irony is that such efforts are likely to undermine, not strengthen, the privacy and security of the information.[133] 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 Honeypot, 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."[134] 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.[135] "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."[136]

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 which continuously improve their security to respond to the ever-growing sophistication of cyber-thieves. As a recent cover feature of the *IEEE Computer Society* magazine observes, "[t]he 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."[137] Information technology associations from Europe, Japan, and the United States have echoed this, arguing

---

[133] DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., THE FALSE PROMISE OF DATA NATIONALISM 1 (2013), *available at* 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.").

[134] Patrick S. Ryan, Sarah Falvey & Ronak Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, 46 COMPUTER 54, 56 (2013).

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

[136] Rohin Dharmakumar, *India's Internet Privacy Woes*, FORBES INDIA (Aug. 23, 2013), http://forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1#ixzz2r0zriZTF.

[137] *Id.*

that "security is a function of how a product is made, used, and maintained, not by whom or where it is made."[138] When Australia was contemplating a rule requiring health data to 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. Microsoft 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."[139]

Indeed, countries pushing for data localization themselves are sometimes hotbeds of cybercrimes. According to experts, "[c]yber security is notoriously weak in Indonesia."[140] Indeed, the nation has been called a "hacker's paradise."[141] 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."[142] Another account suggests that "Brazil is among the main

---

[138] This idea is echoed in submissions from a range of IT consortia. Digital Europe, U.S. Information Technology Industry Council (ITI), Japan Electronics and Information Technology Industries Association (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.

[139] Submission by Microsoft, Personally Controlled Electronic Health Records Bill 2011 – Exposure Draft (Oct. 28, 2011), *available at* http://www.yourhealth.gov.au/internet/yourhealth/blog.nsf/A4CDF04D86373F4ACA2579500012B981/$FILE/38.Microsoft%20Australia,%20part%202%20-%2028%20October.pdf. 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." Submission by CSC to the Standing Comm' on Cmty. Affairs, Personally Controlled Electronic Health Records Bill 2011 – Exposure Draft (Dec. 23, 2011), https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=f9019a89-8166-42a4-b733-3b7d87f4afc3; Josh Taylor, *E-health Law to Block Overseas Access: CSC*, ZDNET (Jan. 9, 2012), http://www.zdnet.com/e-health-law-to-block-overseas-access-csc-1339329216/.

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

[141] *Id.*

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

targets of virtual threats such as malware and phishing."[143] 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."[144] At times, a cyber-theft can begin with a domestic burglary, as in the case of one recent European episode.[145] Or cyber-thefts can 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.[146]

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.

3. 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, whether explicitly or not, are often motivated 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."[147] The

---

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

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

[145] Christopher Thompson, Caroline Binham & Jonathan Guthrie, *ENRC Says Hackers May Have Stolen Data*, FINANCIAL TIMES (May 23, 2013), http://www.ft.com/cms/s/0/e25863cc-c392-11e2-8c30-00144feab7de.html#axzz2so7Tda7r.

[146] Joyce Lee, *South Koreans Seethe, Sue as Credit Card Details Swiped,* REUTERS (Jan. 21, 2014), http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121; 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?_r=0 (last visited Feb. 25, 2014).

[147] *Commission Communication 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), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

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."[148] 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 data facilities and functions" when consistent with other fundamental rights, in order to "ensure cost effectiveness and other efficiencies."[149]

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.[150] The Information Technology Industry Council, an industry association representing more than 40 major Internet companies, argues that Brazilian "in-country data storage requirements would detrimentally impact all economic activity that depends on data flows."[151] The Swedish government agency, the National Board of Trade, recently interviewed fifteen local companies of various sizes across sectors and concluded succinctly: "trade cannot happen without data being moved from one location to another." [152]

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. Critics worry, for example, that the Brazilian data localization requirement would "deny[] Brazilian users access to great services that

---

[148] *Rebuilding Trust in EU-US Data Flows*, *supra* note 36, at 2.

[149] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY-MAKING 8 (Dec. 13, 2011), *available at* http://www.oecd.org/sti/ieconomy/49258588.pdf.

[150] 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/#.

[151] Letter from Information Technology Industry Council Brazil, *supra* note 8. Internet companies in Brazil have largely supported the *Marco Civil*, with the significant exception of this particular provision. For a list of members, see INFORMATION TECHNOLOGY INDUSTRY COUNCIL, http://www.itic.org/about/member-companies.dot (last visited Mar. 10, 2014).

[152] SWEDEN NATIONAL BOARD OF TRADE [KOMMERSKOLLEGIUM], NO TRANSFER, NO TRADE: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFER FOR COMPANIES BASED IN SWEDEN 23 (2014) [hereinafter NO TRANSFER, NO TRADE].

are provided by US and other international companies."[153] Marilia Marciel, a digital policy expert at Fundação Getulio Vargas in Rio de Janeiro, observes, "[e]ven Brazilian companies prefer to host their data outside of Brazil."[154] 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."[155]

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.[156] 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.[157] Building a data center in Brazil costs $60.9 million on average, while building one in Chile and the United States costs $51.2 million and $43 million, respectively.[158] Operating such a

---

[153] Joe Leahy, *Brazil Sparks Furore over Internet Privacy Bill,* FINANCIAL TIMES (Nov. 11, 2013), http://www.ft.com/cms/s/0/5cd5b638-487a-11e3-8237-00144fe abdc0.html #ix zz2qcAAZkRr.

[154] Esteban Israel & Alonso Soto, *Brazil's Anti-spying Internet Push Could Backfire, Industry Says*, REUTERS (Oct. 2, 2013), http://www.reuters.com/article/2013/10/02/us-brazil-internet-idUSBRE9910F120131002.

[155] Original text: "Uma tal obrigação poderá fazer com que os cidadãos, as empresas e outras instituições corram o risco desnecessário de ser excluídos do enorme potencial da economia digital, prejudicando a capacidade do País de criar, inovar, gerar emprego e arrecadar impostos a partir do bom uso da Internet." *BRASSCOM Analisa Marco Civil*, RISK REPORT (Oct. 30, 2013), http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=15079&sid=42.

[156] CUSHMAN & WAKEFIELD, DATA CENTRE RISK INDEX (2013), *available at* http://www.cushmanwakefield.pt/en-gb/research-and-insight/2013/data-centre-risk-index-2013/.

[157] FROST & SULLIVAN, *supra* note 143, at 10. Esteban & Soto, *supra* note 154. Brazil has attempted to address the cost barrier for building local data centers through tax incentives, as part of a broadband infrastructure program, the Special Taxation Regime for the Broadband National Program (*Regime Especial de Tributação do Programa Nacional de Banda Larga*). Decree 7291, published in the Official Gazette on Feb. 18, 2013, Decreto N 7.921, Pág. 2. Seção 1. Diário Oficial da União (DOU) de 18 de Fevereiro de 2013, *available* http://www.jusbrasil.com.br/diarios/50903713/dou-secao-1-18-02-2013-pg-2; Roberta Prescott, *Brazil Signs Tax Relief Measure for Telecom Network Construction*, RCR WIRELESS (Feb. 19, 2013), http://www.rcrwireless.com/americas/20130219/spectrum/brazils-government-signs-decree-relieve-tax-construction-new-telecom-networks/ (last visited Feb. 28, 2014).

[158] Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill*, WALL ST. J. (Nov. 13, 2013),

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.[159] This cost discrepancy is mostly due to high electricity costs and heavy import taxes on the equipment needed for the center.[160] Data centers employ few workers, with energy making up three-quarters of the costs of operations.[161] 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 the riskiest countries for running data centers.[162]

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 are often imported into a country. The diesel generators, cooling systems, servers and power supply devices tend to be imported from a few global suppliers. Ironically, it is often *American* suppliers of servers and other hardware that stand to be the beneficiaries of data localization mandates. One study notes, "Brazilian suppliers of components did not benefit from this [data localization requirement], since the imported products dominate the market."[163] By increasing capital purchases from abroad, data localization requirements can in fact increase merchandise trade deficits. Furthermore, large data farms are enormous consumers of energy, 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 Internet association IdEA, states that '[t]he cost can double easily in Indonesia."[164] 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

---

http://online.wsj.com/news/articles/SB10001424052702304868404579194290325348688 (according to a government-commissioned study seen by *The Wall Street Journal*).

[159] *Id.*

[160] FROST & SULLIVAN, *supra* note 143, at 10.

[161] Rachel A. Dines, *Build or Buy? The Economics of Data Center Facilities*, Forrester, June 27, 2011 (updated July 29, 2011), *available at* http://www.io.com/wp-content/uploads/2013/04/build-or-buy.pdf.

[162] CUSHMAN & WAKEFIELD, *supra* note 156.

[163] *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/.

[164] Avi Tejo Bhaskoro, *Indonesia Ministry Still Insists on Local Data Centers for Online Companies*, DAILYSOCIAL (May 8, 2013), http://en.dailysocial.net/post/indonesian-ministry-still-insists-on-local-data-centers-for-online-companies.

have relied on elsewhere are not fully available yet in Indonesia."[165] Another report suggests that a weak local hosting infrastructure in Indonesia means that sites hosted locally experience delayed loading time.[166] Similarly, as the Vietnamese government attempts to foster entrepreneurship and innovation,[167] localization requirements effectively bar start-ups from utilizing cheap and powerful platforms abroad and potentially handicap Vietnam from "join[ing] in the technology race."[168]

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 to transform Malaysia into a "world-class data centre hub" for the Asia-Pacific region.[169] Brazil hopes to accomplish the same for Latin America, while France seeks to stimulate its economy via a "Made in France" digital industry.[170] 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 will be hampered if other countries engage in similar reactive policies, which "can stimulate the migration of datacenters based

---

[165] 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.

[166] *Id.*

[167] In June 4, 2013, the Ministry of Science and Technology launched the Silicon Valley Project to stimulate the growth of technology startups in Vietnam. Silicon Valley Project, http://www.siliconvalley.com.vn/.

[168] Elisabeth Rosen, *Can Vietnam Create the Next Silicon Valley,* THE ATLANTIC (Feb. 11, 2014), http://www.theatlantic.com/international/archive/2014/02/can-vietnam-create-the-next-silicon-valley/283760/ (last visited Mar. 7, 2014).

[169] EPP 3: Positioning Malaysia as a World-class Data Centre Hub, http://etp.pemandu.gov.my/Business_Services-@-Business_Services_-_EPP_3-;_Positioning_Malaysia_As_A_World-class_Data_Centre_Hub.aspx; Edwin Yapp, *Malaysia Must Fulfil Promises to Boost ICT*, ZDNET, Oct. 18, 2010, http://www.zdnet.com/malaysia-must-fulfil-promises-to-boost-ict-2062203784/; Edwin Yapp, *Malaysia's Data Center Ambition Faces Challenges*, ZDNET, Apr. 28, 2011, http://www.zdnet.com/malaysias-data-center-ambition-faces-challenges-2062208606/ (quoting Fadhlullah Suhaimi Abdul Malek, then-Director for Business Services at Pemandu, the government arm responsible for facilitating the Economic Transformation Program, arguing that "Malaysia has the geographical stability to meet this [growing cloud computing] need" in Asia-Pacific.").

[170] Press Release, The Growing Market for Cloud Computing in France, INVEST IN FRANCE AGENCY (Jan. 2012), http://www.invest-in-france.org/Medias/Publications/1588/cloud-computing-in-France-January-2012.pdf; FRANCE'S 34 SECTOR-BASED INITIATIVES, *supra* note 44.

here, or at least part of them, to other countries…."[171] 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.[172] Then there's the avoidance effect. Rio de Janeiro State University Law Professor Ronaldo Lemos, who helped write the original *Marco Civil*, and currently Director of the Rio Institute for Technology and Society, warns that the localization provision would cause 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."[173] 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 country in Singapore.[174] 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 glasses, driverless cars, and information programs for visually impaired users, are unlikely to develop and grow in Korea. Laws made in the 60s are preventing many venture enterprises from advancing to foreign markets via location/navigation services."[175]

---

[171] Original text: "Em movimento inverso, pode-se estimular a mudança dos Data Centers aqui instalados, ou pelo menos de parte deles, para outros países, em possível prejuízo à arrecadação tributária e à criação de postos de trabalho." *Id.*

[172] 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.

[173] Esteban & Soto, *supra* note 154.

[174] Thu Huong, *Vietnamese 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).

[175] Lee, *supra* note 130; *see also* Lan Goh, *supra* note 129 (quoting Wan Su Lim, the director of the Community Mapping Center, arguing that the 1960s mapping law is preventing many venture enterprises from expanding internationally via location-based services).

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 75 percent of the value added created by the Internet and data flow is in traditional industries, in part through increases in productivity.[176] 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.[177] 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.[178] With data localization mandates, traditional businesses 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.[179] Many companies

---

[176] MCKINSEY GLOBAL INSTITUTE, 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.

[177] MCKINSEY GLOBAL INSTITUTE, DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 55 (2013), *available at* http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx.

[178] *Id.* at 17.

[179] 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, "in reality under the IaaS [Infrastructure as a service] model… the data is not usually "*transferred*" to a third party (ie the vendor)," and thus does not trigger a data transfer obligation, while the SaaS might well trigger such an obligation. Alec Christie, *Cloud Computing and the New Australian Privacy Law*, DLA PIPER (Sept. 24, 2013),

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.[180] 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."[181] A company like Zoho can use Google Apps, while at the same time competing with Google in higher value-added services.[182] 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 so-called "Internet of Things" for both consumers and businesses. Consumer devices include wearable technologies that "measure some sort of detail about you, and log it."[183] Devices such as Sony's Smartband allied with a Lifelog application to track and analyze both physical movements and social interactions or the Fitbit devices 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.[184] A heart monitoring system "collects data from patients and physicians around the world," and uses the anonymized data to "advance cardiac care."[185] 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.[186] Companies are also

---

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.

[180] Jonathan Boutelle, CTO, Slideshare, Presentation at the Amazon and SAP Partner Event (June 17, 2010), *available at* http://www.slideshare.net/jboutelle/slideshare-aws-talk.

[181] *Id.*

[182] Alex Williams, *Zoho Integrates Google Apps and Keeps Step with the Giants*, READWRITE (Dec. 1, 2009), http://readwrite.com/2009/12/01/zoho#awesm=~otx2zoOOYtio6Y.

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

[184] Dan Rowinski, *CES 2014: Connected Homes and Wearables to Take Center Stage,* READWRITE (Jan. 03, 2014), http://readwrite.com/2014/01/03/ces-2014-preview-wearable-technology-4k-tv-connected-home-smartphones-tablets#awesm=~orUIcda6uQcxIa.

[185] ALIVECOR, http://www.alivecor.com/home (last visited Feb. 8, 2014).

[186] 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-

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 data is collected and analyzed remotely.[187] While data about oil flows would hardly constitute personal information, it may well be controlled under data privacy laws that focus on information that may be sensitive on national security grounds. 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.[188] McKinsey even reclassifies data as a new kind of factor of production for the Information Age.[189] 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.

4. 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 and then subsequently with other measures such as the Foreign Intelligence Surveillance Act Amendments Act of

---

2022. JOSEPH BRADLEY, JOEL BARBIER, & DOUG HANDLER, CISCO, EMBRACING THE INTERNET OF EVERYTHING TO CAPTURE YOUR SHARE OF $14.4 TRILLION (2013) http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[187] 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.'").

[188] MCKINSEY GLOBAL INSTITUTE, BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 23, (2011) *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

[189] *Id.*, at 3.

2008. 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.[190] 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.[191] France just recently adopted the law on military programming permitting certain ministries to see "electronic and digital communications" in "real time."[192] 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.[193]

However, 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.

---

[190] Boah Shachtman, *How Gadgets Helped Mumbai Attackers*, WIRED (Dec. 1, 2008), http://www.wired.com/dangerroom/2008/12/the-gagdets-of/; 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.").

[191] 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; 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/.

[192] France Military Programming Law 2013 *supra* note 54, at art. 20.

[193] Dung Nguyen, *Minister Nguyen Bac Son: Decree 72 Protects the Interests of Internet Users* [*Bộ Trưởng Nguyễn Bắc Son: Nghị định 72 Bảo Vệ Lợi Ích Người Dùng Internet*], INFONET.VN (Aug. 31, 2013) (Vietnam) (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."); "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.")

Data localization will not necessary 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 the data localization rules, while others will simply ignore them. 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 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.[194] 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…"[195]

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 41 countries including the United States, France and Germany,[196] obliges Member States to adopt and enforce laws against cybercrimes and to provide "mutual assistance" to each other in enforcing cyber-offenses.[197] Many states have entered into specific Mutual Legal

---

[194] HOGAN LOVELLS WHITE PAPER, *supra* note 127.

[195] The study examines the laws of the following countries: Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, the United Kingdom and the United States.

[196] Members to the Convention on Cybercrime are Albania, Argentina, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Malta, Mauritius, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, and United States. Council of Europe, Convention on Cybercrime, Opening for Signature, Status as of 19/2/2014, CETS No. 185, http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=185&CL=ENG (listing all states that have signed as of February 19, 2014).

[197] Council of Europe, Convention on Cybercrime, art. 25(1), Nov. 23, 2001, Budapest, ETS No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Assistance Treaties (MLATs) with foreign nations. These treaties establish a process that protects the rights of individuals, yet give governments access to data held in foreign jurisdictions. The United States currently has MLATs 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.[198] The U.S. also entered into a Mutual Legal Assistance Agreement (MLAA) with China and Taiwan. 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."[199] 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.[200] 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."[201] At the same time, there are procedural requirements to help ensure that the information gathering is supporting a proper governmental investigation. For example, the Section 17 of the US-Germany MLAT provides that the government requesting assistance must do so in writing,

("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.").

198 U.S. DEPT. OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (INCSR) (2012), *available at* http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

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

200 INT'L BAR ASS'N, THE ALLEGED TRANSNATIONAL CRIMINAL: THE SECOND BIENNIAL INTERNATIONAL CRIMINAL LAW SEMINAR 374-75 (Richard D. Atkins ed. 1995).

201 Agreement on Mutual Legal Assistance between the European Union and the United States of America, art. 9(2)(b), July 19, 2003, T.I.A.S. No. 10-201.1, 2003 O.J. (L 181/34); HOGAN LOVELLS WHITE PAPER, *supra* note 127.

must specify the evidence or information sought, authorities involved, and applicable criminal law provisions, etc.[202]

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.[203] Similarly, the European Commission has recently stressed that the rebuilding of trust in the US-EU relationship must focus in part on a commitment to use legal frameworks such as the MLATs.[204] 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.

5. 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."[205] 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 are 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 for authoritarian regimes to suppress their citizens from both sharing and learning information, though not impossible.[206] 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 or not 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 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," that is also safe from

---

[202] Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Germany, Nov. 16, 2004, T.I.A.S. 09-1018, Oct. 14, 2003, S. TREATY DOC. No. 108-27 (Nov. 16, 2004), *available at* http://www.gpo.gov/fdsys/pkg/CDOC-108tdoc27/pdf/CDOC-108tdoc27.pdf.

[203] INT'L CHAMBER OF COMMERCE, *supra* note 199, at 6.

[204] *Rebuilding Trust in EU-US Data Flows*, *supra* note 36, at 8.

[205] Anupam Chander, *Googling Freedom*, 99 CAL. L. REV. 1, 20 (2011).

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

[stuxnet] cyber-attacks and dangers posed by using foreign networks.[207] 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."[208] An Iranian journalist agreed, "This is a ploy by the regime. . . . that only allows you to visit permitted websites."[209] 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."[210]

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.[211] 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,"[212] 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."[213] One observer argues, "This is a law that has been established for selective persecution. This is a law that will be used against certain people who have become a thorn in the side of the

---

[207] Christopher Rhoads & Farnaz Fassihi, *Iran Vows to Unplug Internet*, WALL ST. J. (May 28, 2011), http://online.wsj.com/news/articles/SB10001424052748704889404576277391449002016?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704889404576277391449002016.html.

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

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

[210] *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.

[211] Huong, *supra* note 174 (noting that Yahoo*!*'s servers serving Vietnam are based in Singapore).

[212] *Vietnam Rebuffs Criticism of "Misunderstood" Web Decree*, REUTERS (Aug. 6, 2013), http://www.reuters.com/article/2013/08/06/vietnam-internet-idUSL4N0G72IA20130806.

[213] *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.

authorities in Hanoi."[214]

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."

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 N.S.A. surveillance to justify increasing control over companies such as Facebook and Google.[215] Such rules have led critics to worry about increasing surveillance powers of the Russian state.[216] Critics caution, "In the future, Russia may even succeed in splintering the web, breaking off from the global Internet a Russian intranet that's easier for it to control."[217] Even though officials describe such rules as being anti-terrorist, others see a more sinister motive. The editor of Agentura.ru, Andrei Soldatov, believes that Zheleznyak's proposal is motivated by the

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

[215] Andrew E. Kramer, *N.S.A. Leaks Revive Push in Russia to Control Net*, N.Y. TIMES (July 14, 2013), http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?pagewanted=1&_r=1.

[216] Andrew Soldatov & Irina Borogan, *Russia's Surveillance State*, 30 WORLD POL'Y J. 23-30 (2013), *available at* http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

[217] *Id.*

government's desire to control internal dissent.[218] 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."[219] Begtin warns, "In fact, we are moving very fast down the Chinese path."[220]

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.[221] The proposal for a German "Internetz" has drawn worries that national routing would require deep packet inspection, raising fears of extensive surveillance.[222] 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 (the *Bundesnachrichtendienst*).[223] 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.[224]

---

[218] 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.

[219] Maria Makutina, *Lawmakers Seek to Bolster Russia's Internet Sovereignty*, RUSSIA BEYOND THE HEADLINES, (June 21, 2013), http://rbth.ru/politics/2013/06/21/lawmakers_seek_to_bolster_russias_internet_sovereignty_27365.html.

[220] *Id.*

[221] 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 (2002).

[222] Richard Adhikari, *Deutsche Telekom Pitches NSA-Free German Internet*, TECH NEWS WORLD (Oct. 26, 2013), http://www.technewsworld.com/story/79286.html. On deep packet inspection, see Hal Abelson, Ken Ledeen & Chris Lewis, *Just Deliver the Packets*, *in* ESSAYS ON DEEP PACKET INSPECTION, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2009), http://www.priv.gc.ca/information/research-recherche/2009/ledeen-lewis_200903_e.asp.

[223] *The German Prism: Berlin Wants to Spy Too*, SPIEGEL (June 17, 2013), http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html.

[224] *India: New Monitoring System Threatens Rights*, HUMAN RIGHTS WATCH (Jun. 7, 2013), http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights (last visited Mar. 7, 2014) ("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. 9, 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 policy level prior to its operation, as its current

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."[225] 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.[226] 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.[227] 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.

---

vagueness and excessive control over communications can create a potential for unprecedented abuse.").

[225] 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); Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013).

[226] Molly 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).

[227] 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 on Cloud Computing, 01037/12/EN, July 1, 2012. ISO 27001 is a well-accepted international standard for Information Security Management Systems. Wikipedia, *ISO/IEC 27001:2005*, http://en.wikipedia.org/wiki/ISO/IEC_27001:2005.