PUBLICATION

Telecom Globalization and Deregulation Encounter U.S. National Security and Labor Concerns

Warren G. Lavey

June 2007

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Warren G. Lavey, Esq., is a partner in the law firm Skadden, Arps, Slate, Meagher & Flom LLP, and former assistant to the chief, Common Carrier Bureau, Federal Communications Commission. He holds B.A. and M.S. degrees from Harvard University; a Diploma Econ. from Cambridge University; and a J.D. from Harvard Law School.

ISBN 1-879716-80-1 **P-07-2**

Acknowledgments

I am grateful for the assistance of Joan Summers, the helpful comments of Anthony Oettinger, Ted Carlson, David Gross, and Ivan Schlager, as well as the following reviews arranged through the Harvard Program on Information Resources Policy: Gianmatteo Arena, Scott Bradner, Marcus Breen, Jean-Pierre Chamoux, James Cortada, C. Derrick Huang, Sean Kanuck, Wolter Lemstra, Richard Levins, Albert Lubarsky, Lionel Olmer, Viktor Mayer-Schoenberger, Leslie Orband, John Rim, and Peter Shapiro. The author represented Alcatel, Dubai Aerospace Enterprise, Global Crossing Ltd., Maher Terminals Holdings Corp. and Toshiba Corp. on national security reviews. Errors are mine alone.

Contents

Page

Executive Summary

This paper reviews three sets of recent company-specific restrictions on non-U.S. ownership and global operations of U.S. telecommunications services and equipment businesses. These restrictions were imposed through reviews of acquisitions by the U.S. Committee on Foreign Investment in the United States and the Federal Communications Commission, and are based on concerns about U.S. national security and jobs. A wide range of actions by the U.S. government have fostered open borders in the telecommunications sector for ownership, services and equipment, reflecting policy directions which differ from the thrust of these recent restrictions. Other governments have objected to these types of restrictions as U.S. barriers to trade and investment. To achieve greater national security without these threats to globalization policies, the U.S. government should adopt a more uniform approach to protections applicable to U.S.-owned as well as non-U.S.-owned firms in this sector. Industry-wide protections are being pursued in other sectors through U.S. legislation and regulatory rules.

Chapter One

Introduction

The last Friday in 2006 was hardly an auspicious day for the U.S. federal government to single out the U.S. telecommunications industry by erecting barriers to the globalization of businesses. Many government offices and businesses closed early that day leading into the three-day holiday weekend. Moreover, the U.S. telecom industry had not lobbied for national protectionist barriers and was quite healthy; revenues for the U.S. telecom industry grew in 2006 at about 2.7%, shaking off the multi-year slump of excess capacity and slacking demand.[1] U.S. telecom carriers were part of an increasingly global service industry; international telecom traffic rose as Internet usage and broadband connections continued to expand in all countries.[2]

On December 29, 2006, the Federal Communications Commission (FCC) adopted an order with a condition opposing the globalization of operations for U.S. telecom carriers.[3] The order approved the merger of AT&T Inc. and BellSouth Corp. After intense pressure from the two Democratic commissioners, the merging companies agreed to various conditions on their operations in order to obtain this approval. While the companies accepted the costs of these conditions in the context of their expected net present value of $18 billion in merger synergies,[4] some of the conditions implicated broader public policies.

Among the conditions for FCC approval of this merger is a commitment by the merged company to repatriate 3,000 jobs that were outsourced by BellSouth outside the United States.[5]

---

[1] See Written Statement of Federal Communications Commission Chairman Kevin J. Martin before the Senate Committee on Commerce, Science and Transportation at 3 (Feb. 1, 2007) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270192A1.pdf) ("In 2006, the communications industry experienced record growth and, by most measures, almost all sectors have rebounded remarkably.... Markets and companies are investing again, job creation in the industry is high...."); Citigroup Analyst Report, "Telecommunications Services: EMT Conference and 4Q Preview—Signals for a Telecom Renaissance?" at 1 (Jan. 4, 2007).

[2] See FCC News Release, "International Bureau Releases 2005 Year-End Circuit Status Report for U.S. Facilities-Based International Carriers" (Jan. 19, 2007) (56 percent growth in use of U.S.-international facilities for international calls, private lines services, and other services from the U.S. in 2005); FCC Public Notice, "FCC Releases 2004 International Traffic Data" (Mar. 14, 2006) at 1 (minutes of facilities-based and facilities-resale traffic between the United States and other countries increased 32.5 percent from 2003 to 2004).

[3] FCC News Release, "FCC Approves Merger of AT&T Inc. and BellSouth Corporation; Significant Public Interest Benefits Likely to Result" (Dec. 29, 2006) ("AT&T/BellSouth FCC Release").

[4] AT&T Inc. filing with the Securities and Exchange Commission (SEC) pursuant to Rule 425, "AT&T and BellSouth to Merge" at 3 (Mar. 7, 2006).

[5] AT&T/BellSouth FCC Release, attached letter from AT&T at 2 ("AT&T/BellSouth is committed to providing high quality employment opportunities in the U.S. In order to further this commitment, AT&T/BellSouth will repatriate 3,000 jobs that are currently outsourced by BellSouth outside of the U.S. This repatriation will be completed by December 31, 2008. At least 200 of the repatriated jobs will be located within the New Orleans, Louisiana MSA [metropolitan statistical area].").

Democratic Commissioner Michael Copps was unmoved by the cost savings BellSouth had found from such outsourcing as well as the global flow of telecom technologies. Instead, in an act favoring organized labor (an important constituent in Democratic politics), Copps made protecting U.S. jobs an important part of the public interest in U.S. communications regulations, and suggested that U.S. businesses must look within the nation's borders for obtaining innovative telecom technologies and associated services:[6]

> The revolution in communications that we are witnessing must not come at the expense of America's hard-working communications workers. Indeed, these high-quality, dedicated, and organized workers are key to bringing us the next generation of communications services.

This comes after years of battles by the FCC—under both Democratic and Republican administrations—against barriers imposed by the United States and countries around the globe to foreign investment in telecom carriers and to opportunities for telecom companies to operate on a transnational basis.[7]

---

[6] Statement of Commissioner Michael J. Copps, Concurring, Re: In the Matter of AT&T and BellSouth Corporation Application for Transfer of Control (WC Docket No. 06-74) at 6 (Dec. 29, 2006) ("Copps Statement"). Neither the other Democratic commissioner nor any Republican commissioner addressed the jobs repatriation condition in the statements on the AT&T/BellSouth merger approval. See Joint Statement of Chairman Kevin J. Martin and Commissioner Deborah Taylor Tate (WC Docket No. 06-74) (Dec. 29, 2006), Statement of Commissioner Jonathan S. Adelstein, Concurring (WC Docket No. 06-74) (Dec. 29, 2006). For different views, see generally Kimmitt, "Why Job Churn is Good," *Washington Post* A17 (Jan. 23, 2007) (available at www.washingtonpost.com/wp-dyn/content/article/2007/01/22/AR2007012201089.html) (Deputy Secretary of the Treasury; "This flexibility of our job market is one key reason the United States successfully competes in an increasingly interconnected global economy.... The dynamism of our workforce helps keep the United States competitive because it increases not only the number of jobs available but also the productivity of those holding jobs."); Business Roundtable, "Securing Growth and Jobs: Improving U.S. Prosperity in a Worldwide Economy" (Mar. 2004) (available at www.businessroundtable.org/pdf/20040330000brsourcing.pdf); Global Insight (USA), Inc., *The Comprehensive Impact of Offshore IT Software and Services Outsourcing on the U.S. Economy and the IT Industry* (Mar. 2004) (available at www.itaa.org/itserv/docs/execsumm.pdf); P. McDougall, "Indian Outsourcer Breaks $1 Billion Quarterly Barrier" (Jan. 16, 2007)(available at www.informationweek.com/outsourcing/showArticle.jhtml?articleID=196901052).

[7] See The White House, *A National Security Strategy for the New Century* 17 (May 1997) (available at http://clinton2.nara.gov/WH/EOP/NSC/Strategy/) ("We have completed the Information Technology Agreement which goes far toward eliminating tariffs on high technology products and amounts to a global annual tax cut of $5 billion. We also concluded a landmark [World Trade Organization] WTO agreement that will dramatically liberalize world trade in telecommunications services. Under this agreement, covering over 99 percent of WTO member telecommunications revenues, a decades old tradition of telecommunications monopolies and closed markets will give way to market opening deregulation and competition principles championed by the United States."); The White House, T*he National Security Strategy of the United States of America* 5 (Sep. 2002) (available at www.whitehouse.gov/nsc/nss.pdf) (commitment to free trade and free markets); FCC International Bureau, "Foreign Ownership Guidelines for FCC Common Carrier and Aeronautical Radio Licenses" (DA 04-3610) (Nov. 17, 2004); FCC International Bureau, "Report on International Telecommunications Markets 2000 Update" (DA 01-117) (May 4, 2001); FCC News Release, "Entry into Force of WTO [World Trade Organization] Telecom Agreement" (Jan. 26, 1998) (available at www.fcc.gov/Bureaus/International/News_Releases/1998/nrin8001.html) (Chairman William Kennard: "This agreement allows telecommunications consumers worldwide to enjoy the benefits of improved competition in basic and

The FCC's repatriation condition to the AT&T-BellSouth merger is in sharp contrast to the contemporaneous news of several developments in globalizing U.S. manufacturing, businesses and investments. On that same day, Chrysler Group, a large U.S. business that at that time was part of the German company DaimlerChrysler AG, said that it could not make money by manufacturing small cars in the United States due to high labor and other costs; it announced a deal with China's Chery Automobile Co. for the Chinese manufacturer to build small cars to be sold at Chrysler dealerships in the United States, Europe, and elsewhere under a Chrysler brand.[8] Moreover, on that day *The Wall Street Journal* reported that the U.S. financial services firm Marsh & McLennan Companies, Inc. agreed in principle to sell Putnam Investments to Power Corp. of Canada for $3.9 billion; Power Corp. beat out two other foreign firms, the United Kingdom's Amvescap and Italy's UniCredito Italiano, in the bidding for the Boston-based asset-management company.[9] That day also saw the U.S. Treasury Department announce that Americans increased their portfolio holdings of foreign securities by 21.7% in 2005 to a total of $4.61 trillion.[10]

The FCC's action on that day was not an isolated political nod to U.S. labor unions. This report reviews three sets of restrictions on foreign controls over and foreign operations of U.S. telecom businesses adopted in the last two months of 2006. Two such restrictions arose pursuant to national security reviews of foreign acquisitions by the Committee on Foreign Investment in the United States (CFIUS—a coordinated effort of the Departments of Treasury, Homeland Security, Justice, Defense, State and Commerce as well as the National Security Council, Office of Science and Technology Policy, U.S. Trade Representative, National Economic Council, Council of Economic Advisors and Office of Management and Budget).[11] The other set of restrictions is in the FCC order on the AT&T/BellSouth merger.

---

advanced telecommunications services. It will increase investment and competition in the United States, leading to lower prices, enhanced innovation and better service. At the same time, market access commitments from major trading partners will provide U.S. service suppliers opportunities to expand abroad."); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, 12 FCC Rcd 23891 (1997).

[8] AP, "Chrysler Signs China Car Deal" (Dec. 29, 2006) (available at http://biz.yahoo.com/ap/061229/chrysler_chery.html?v=4). See generally "Behind the Asian outsourcing phenomenon", *McKinsey Quarterly* (Feb. 21, 2004) (available at http://news.com.com/Behind+the+Asian+outsourcing+phenomenon/2030-1069_3-5162352.html); "The Problem with Made in China," *The Economist* (Jan. 11, 2007) (available at http://www.economist.com/business/displaystory.cfm?story_id=8515811).

[9] See CNBC, "Power Corp. to Buy Marsh & McLennan's Putnam" (Dec. 29, 2006) (available at http://www.cnbc.com/id/16389766).

[10] See MarketWatch, "U.S. Holdings of Foreign Securities Up 21.7% in 2005" (Dec. 29, 2006) (available at http://www.marketwatch.com/news/story/us-holdings-foreign-securities-up/story.aspx?guid=%7B97F10A0F%2DCB98%2D42FD%2D8E40%2D1BF41E1E4DB9%7D).

[11] See Section 5021 of the Omnibus Trade and Competitiveness Act of 1988, amending Section 721 of the Defense Production Act of 1950 ("Exon-Florio Provision"); Executive Order 11858 (1975); Executive Order 12661(1988);

The analysis is not intended to challenge the national security and employment security concerns and other public policies underlying these restrictions. Instead, the intent is to contrast these restrictions with the efforts by Congress, the FCC and other federal agencies to deregulate and globalize the telecom industry, and to point out some of the possible economic costs of these restrictions. In addition, this paper contrasts the U.S. government's use of transaction-specific restrictions in the telecommunications sector with the industry-wide legislation and regulatory rules applying similar restrictions to several other infrastructure industries. The hope is to focus attention on developing a coherent approach to these issues.

Chapter Two of this report describes CFIUS reviews and related agreements for two foreign acquisitions of U.S. businesses, one a telecommunications carrier/Internet services provider and the other a manufacturer of telecommunications equipment. The conditions for approval of each transaction are analyzed in the context of related policies, laws, orders and other governmental actions. Next, **Chapter Three** addresses the labor condition, and lack of national security conditions, in the FCC's order approving the AT&T/BellSouth merger, again in the context of related governmental actions. To further establish the context for these U.S. restrictions, **Chapter Four** describes some foreign responses, reviews and restrictions. Then, **Chapter Five** presents several examples of efforts by the U.S. government to address national security vulnerabilities through industry-wide measures, regardless of whether the business is U.S.-owned or foreign-owned. Theses vulnerabilities and measures are similar to those addressed through the transaction-specific CFIUS reviews that are limited to foreign acquisitions. Finally, **Chapter Six** presents the conclusion on problems with the U.S. government's actions on the three transactions described in this report.

This report makes the following findings regarding U.S. policies and actions: (1) conditions imposed on merging companies to promote national security and labor concerns lack industry-wide application, and conditions required by the U.S. government for some transactions are opposed to legislation and regulations adopted with an industry-wide perspective; (2) the evaluation and negotiation of merger conditions for foreign acquirers of U.S. businesses involve different government entities and processes than for domestic acquisitions, leading to inconsistent conditions even with regard to what may be viewed as industry best practices for national security; (3) Congress, the FCC and other federal agencies have not acted to promote consistency in national security and labor practices across competing domestic and foreign-owned providers in the telecommunications sector, resulting in security vulnerabilities as well as the risks of deterring foreign investments in the United States and countermeasures by foreign governments against U.S. companies; and (4) Congress and agencies have adopted industry-wide legislation and rules applying national-security measures, without singling out foreign-owned firms, in several infrastructure industries, including marine ports, airports, and nuclear power plants but not in the telecommunications sector.

Executive Order 12860 (1993); 31 CFR Part 800.

Chapter Two

National Security Reviews of Foreign Acquisitions of U.S. Telecom Businesses

There are many tensions between areas of communications policies and national security concerns. Yet, U.S. laws and political leaders have long recognized the national security importance of U.S. telecommunications carriers and the need to integrate national security objectives in communications policies. For example, the Communications Act of 1934, as amended, declares the policy of regulating wire and radio communications for, among other purposes, the national defense and to promote safety of life and property.[1] Several other laws establish procedures and requirements for telecommunications carriers to assist law enforcement and national security agencies by implementing wiretaps and providing call records.[2] The increased focus on national security after 9/11/2001 included actions highlighting the importance of telecommunications carriers in efforts to safeguard the country against terrorists (through wiretaps and call records)[3] and as providers of critical infrastructure. In releasing a national security strategy report in 2003, President George W. Bush referred to the reliance of U.S. businesses, government operations and national defense on "an interdependent network of information technology infrastructures called cyberspace."[4]

The heart of the legislation, executive orders and rules creating and guiding CFIUS reviews is the belief that some proposed foreign acquisitions of U.S. businesses may pose threats to U.S. national security that would not exist if such businesses continued under U.S. ownership and control.[5] CFIUS has reviewed a range of foreign investments in U.S. telecom businesses in recent years. Among the landmarks in CFIUS's dealings with telecom transactions are the conditions adopted for Japanese NTT Communications' acquisition of Internet services provider Verio, Inc.

---

[1] 47 U.S.C. §151.

[2] See Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 229, 1001 *et seq.*; Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62; USA PATRIOT Act of 2001, 115 Stat. 272 (2001).

[3] In addition to passage of expanded authority for wiretaps and call records in the USA PATRIOT Act of 2001, this issue was highlighted in 2005 and 2006 with disclosure of a program by the National Security Agency involving some large telephone carriers and interceptions of international telephone and Internet communications without a warrant or other judicial approval. See Terkel v. AT&T, 441 F. Supp.2d 899 (N.D. Ill. 2006); Hepting v. AT&T, 439 F. Supp.2d 974 (N.D. Cal. 2006); ACLU v. NSA, 438 F. Supp.2d 754 (E.D. Mich. 2006); In re National Security Agency Telecommunications Record Litigation, MDL No. 06-1791 (VRW) (N.D. Cal.).

[4] White House Report, The National Strategy to Secure Cyberspace at iii (Feb. 2003) (available at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf) ("National Strategy"). See also Chapter Two, note 21.

[5] See Chapter One, note 11; Transcript of [Treasury] Secretary [Henry M.] Paulson's Remarks at Forum on International Investment at 2 (May 10, 2007) (available at http://www.treasury.gov/press/releases/hp398.htm) ("Paulson") ("The CFIUS process applies only when a transaction may be related to national security, and that is a very small percentage of foreign investment….When a transaction may relate to national security, our policy remains as it has been since CFIUS was created – to ensure national security first while keeping America open to investment.").

(2000); conditions adopted for German Deutsche Telekom's acquisition of VoiceStream Wireless Corp. (2001); and rejection of Hong Kong Hutchison Telecommunications' attempt to acquire a 31 percent interest in Global Crossing Ltd., followed by conditions adopted in Singapore Technologies Telemedia Pte Ltd's acquisition of a 61 percent interest in Global Crossing (2003).[6]

In mid-2006, CFIUS was operating in a highly-charged political environment surrounding its reviews and foreign acquisitions. There was a political furor over the proposed acquisition of U.S. port operations by a Dubai entity which had cleared CFIUS review, leading the foreign company to drop the U.S. business from the acquisition;[7] focus on a bid by the government-backed China National Overseas Oil Corporation for Unocal, which was withdrawn after an outpouring of Congressional opposition;[8] a negative report by the General Accountability Office on the thoroughness of CFIUS's reviews and conditions it imposed on transactions;[9] and numerous bills pending in both houses of Congress to revise the standards and review processes for foreign acquisitions.[10]

---

[6] See J. Lewis, "New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure and Communications Interception," 57 *Fed. Com. L. J.* 457 (2005) ("Lewis").

[7] See J. Holzer, "Was the Law Followed on Dubai Ports Deal OK?" (Feb. 23, 2006) (available at http://www.forbes.com/business/2006/02/22/logistics-ports-dubai-cx_jh_0223cfius.html); CNN, "Key Questions About the Dubai Port Deal" (Mar. 6, 2006) (available at http://www.cnn.com/2006/POLITICS/03/06/dubai.ports.qa/index.html); S. Kirchgaessner, "Fear Grows Over New Dubai Revolt" (Mar. 21, 2006) (available at http://www.ft.com/cms/s/c8f7de22-b91c-11da-b57d-0000779e2340.html).

[8] See S. Cohen, "Lawmakers Rip CNOOC's Unocal Bid" (July 13, 2005) (available at http://www.marketwatch.com/News/Story/Story.aspx?guid=%7B965D9D52-8989-4FDF-8283-54F1B4A80271%7D&siteid=mktw&dist=&print=true&dist=printBottom); D. Barboza, "China Backs Away from Unocal Bid" (Aug. 3, 2005) (available at http://www.iht.com/articles/2005/08/02/business/unocal.php); Note, "From Fretting Takeovers to Vetting CFIUS: Finding a Balance in U.S. Policy Regarding Foreign Acquisitions," 39 *Vand. J. Transnat'l L.* 1303, 1319-26 (2006).

[9] U.S. General Accountability Office, "Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness," GAO-05-686 (Sept. 2005). See also U.S. General Accountability Office, "Defense Trade: National Security Reviews of Foreign Acquisitions of U.S. Companies Could be Improved," GAO-07-611T (Mar. 2007) ("GAO 2007 Report").

[10] See B. McConnell, "Battle Likely After Rival Bills for Foreign Merger Oversight Reform Approved," *The Deal* (July 28, 2006) (available at http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1153991138266); S. Canner, "A Layman's Guide to CFIUS Reform" (July 2006) (available at http://www.uscib.org/index.asp?documentID=3506); S. Kirchgaessner, "CFIUS Reform Back in Spotlight" (Aug. 23, 2006) (available at http://www.ft.com/cms/s/1523f970-32d0-11db-87ac-0000779e2340.html); Treasury Dep. Sec. Robert M. Kimmitt, "CFIUS Reform and International Investments: Balancing Security and Investment" (Oct. 27, 2006) (available at http://www.ustreas.gov/press/releases/hp155.htm); Testimony of Assistant Secretary for International Affairs Clay Lowery Before the House Financial Services Subcommittee on Domestic and International Monetary Policy, Trade and Technology On Reform of CFIUS (May 17, 2006) (available at http://www.ustreas.gov/press/releases/js4269.htm) ("Sound legislation can ensure that the Committee reviews transactions thoroughly, protects the national security, conducts its affairs in an accountable manner, and avoids creating undue barriers to foreign investment in the United States.").

To understand some of the concerns addressed by CFIUS in telecom transactions and the resulting restraints on globalization and regulatory burdens, consider the conditions announced in the last two months of 2006 for two transactions: (A) the sale of a controlling interest in Telecomunicaciones de Puerto Rico, Inc. (TELPRI) by Verizon Communications, Inc. to América Móvil, S.A. de C. V. (a Mexican company),[11] and (B) the merger of Lucent Technologies, Inc. and Alcatel (a French company).[12]

2.1 Restrictions on Globalization of Operations for a Telecom Services Provider to Promote U.S. National Security

2.1.1 Background on the TELPRI Transaction

To clear CFIUS review, América Móvil and TELPRI entered into a Security Agreement with the Departments of Justice and Homeland Security in December 2006.[13] The provisions of this agreement illustrate a broad, penetrating role for these executive branch agencies and a nationalistic approach which conflicts with the actions of Congress, the FCC and other federal agencies on deregulation and globalization over the past decade.

As background, in 2006 TELPRI served approximately 1.1 million landline and 500,000 wireless subscribers in Puerto Rico[14] (which is treated as part of the United States for purposes of CFIUS and FCC jurisdiction). América Móvil served approximately 100 million wireless

---

[11] See "Verizon to Sell Caribbean and Latin American Telecom Operations in Three Transactions Valued at $3.7 Billion," Verizon Press Release (Apr. 3, 2006) (available at http://investor.verizon.com/news/view.aspx?NewsID=731); FCC Public Notice, "América Móvil, S.A. de C.V., Verizon Communications Inc., and Subsidiaries of Telecomunicaciones de Puerto Rico, Inc. Seek FCC Consent to Transfer Control of Licenses and Authorizations and Request a Declaratory Ruling on Foreign Ownership," DA 06-1245 (June 14, 2006).

[12] See "Alcatel and Lucent Technologies to Merge and Form World's Leading Communication Solutions Provider," Alcatel and Lucent Technologies, Inc. Joint Press Release (Apr. 2, 2006) (available at http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4x3MQ3VL8h2VAQAgjlFVg!!) ("Alcatel/Lucent Announcement").

[13] Department of Justice, FBI and Department of Homeland Security, Petition to Adopt Conditions to Authorizations and Licenses, filed in FCC WT Docket No. 06-113, Verizon Communications, Inc., Transferor and América Móvil, S.A. de C.V., Transferee (Dec. 15, 2006) (available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518713387) ("TELPRI Security Agreement"). This agreement is attached as Exhibit 1 to the FCC's order approving the transaction. Verizon Communications, Inc., Transferor, and América Móvil, S.A. DE C.V., Transferee, FCC 07-43 (Mar. 26, 2007) ("Verizon/AM Order").

[14] Application filed by América Móvil and Verizon Communications in FCC WT Docket No. 06-113, Overview of Transaction/Petition for Declaratory Ruling/Request Procedural Considerations at 5, Public Interest Statement at 2-3 (May 9, 2006) (available at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518360185) ("TELPRI Application").

subscribers and 2 million landline subscribers in fourteen countries in the Americas, and was under common control with the largest provider of wireline services in Mexico.[15]

In applying to the FCC for approval of the transaction, América Móvil claimed that it "will be able to take advantage of economies of scale and scope with its existing operations in serving Puerto Rico."[16] The examples provided in this application included lower costs for procuring some types of equipment through volume discounts. América Móvil also pointed to its expertise in operating telecom networks, upgrading technologies and designing telecom service offerings.

Regional operations offer carriers opportunities for integration and consolidation, resulting in savings in operating expenses and capital expenditures. Some providers across multiple countries in the Americas point to savings from integrated billing services, network monitoring and fault correction, network facilities, network planning and applications development.[17] Moreover, it is common for carriers serving multiple regions in a country to implement centralized network operating, customer service, switching, Internet peering and hosting centers as well as other consolidated operations.[18]

---

[15] Id., Overview of the Transaction at 4, Public Interest Statement at 3.

[16] Id., Public Interest Statement at 1, 3-5.

[17] See América Móvil, S.A. de C.V. 2005 Form 20-F at 32 (filed with the SEC on June 30, 2006) ("América Móvil 2005 Form 20-F") ("Speedy Movil, S.A. de C.V. is a Mexican company that develops mobile data solutions for SMS, wireless Internet (WAP) and voice-activated data applications for Telcel and our other subsidiaries and investments"); Centennial Communications Corp. 2005 Form 10-K/A, Amendment No. 1 at 10 (filed with the SEC on Dec. 12, 2005) ("Centennial") ("In accordance with our strategy of developing market clusters, we have selected wireless switching systems that are capable of serving multiple markets with a single switch. Where we have deemed it appropriate, we have implemented microwave links and fiber connections in our U.S. wireless telephone systems and Caribbean integrated communication system, which provide ongoing cost efficiency and generally improve system reliability.... We have outsourced with Convergys Information Management Group, Inc...., a network management and operations support systems provider, to provide billing services, facilitate network fault detection, correction and management, performance and usage monitoring and security for our wireless operations throughout our company."); BellSouth Corp. 1999 Form 10-K at 14 (filed with the SEC on Mar. 2, 2000) ("We are developing business relationships and regional synergies among our Latin American joint ventures....We are also creating our own international network as well as regional switching centers, to be used to offer voice and data international long distance services linking our wireless joint ventures and other operations in Latin America when permitted by local law."); Telefonica Moviles, S.A. 2005 Form 20-F at 18 (filed with the SEC on Apr. 12, 2006) ("We believe that our larger scale, the regional integrated management of our operations in Latin America and the integration of the BellSouth mobile operators in 2004 and 2005 will lead to material savings in areas like handset and equipment procurement, infrastructure and IT systems sharing and advertising.").

[18] See Centennial, *supra*, at 9 (wireless operations in Indiana, Michigan, Texas, Louisiana and Mississippi, with one centralized customer service center and local customer support facilities); Dobson Communications Corp. 2005 Form 10-K at 4, 10, 12 (filed with the SEC on Mar. 16, 2006) (wireless operations in sixteen states; "We have integrated the operations of numerous acquired wireless systems into our existing operations to achieve economies of scale. We have generated efficiencies from the consolidation and centralized control of pricing, customer service, marketing, system design, engineering, purchasing, financial, administrative and billing functions... A large portion of these [customer]services are provided by our national customer service centers, which service all of our markets. At December 31, 2005, we operated three customer service centers, which are located in Oklahoma City, Oklahoma, Duluth, Minnesota and Youngstown, Ohio... Our network operations are monitored by regional network personnel and

2.1.2 Security Agreement for the TELPRI Transaction

Most conditions imposed on foreign acquisitions pursuant to CFIUS reviews are not publicly disclosed. However, CFIUS's Security Agreement for the TELPRI transaction (hereafter "Security Agreement") was filed publicly with the FCC with a request that the FCC make compliance with this agreement a condition for its approval of the transfer of control over TELPRI.[19]

The Security Agreement recites several reasons why the CFIUS agencies sought restrictions in connection with the foreign acquisition of TELPRI, including:[20]

- U.S. communications systems are essential to the ability of the U.S. Government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;
- the U.S. Government has an obligation to the public to ensure that U.S. communications and related information are secure in order to protect the privacy of U.S. persons and to enforce the laws of the United States;
- it is critical to the well being of the nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States; and
- TELPRI subsidiary [Puerto Rico Telephone Company, Inc.] provides telecommunications services to federal government agencies and the Puerto Rico National Guard.

Put differently, the U.S. government appears to be concerned that the foreign owner of the telecom services provider could, among other things, (1) disclose to foreign governments or persons information on U.S. telecom subscribers and their calls; (2) disclose to foreigners information on U.S. law enforcement activities such as wiretaps and requests for call records; (3) impair on behalf of foreigners such U.S. law enforcement activities; (4) disrupt telecom services used by U.S. government entities and other U.S. persons; or (5) increase the risk of a foreigner's

---

our vendors, who provide monitoring on a real-time basis for items, including alarm monitoring, power outages, tower lighting problems and traffic patterns.").

[19] See note 13 to this chapter. In a separate letter to representatives of the Department of Defense, América Móvil made further commitments to safeguard the Department's ability to realign military installations and to ensure appropriate security controls remain in place to protect sensitive military communications. Petition to Adopt Conditions Filed by Department of Defense in WT Docket No. 06-113 (Dec. 19, 2006) (available at gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518714878). This agreement is attached as Appendix C to the FCC's order approving the transaction. Verizon/AM Order, *supra*.

[20] TELPRI Security Agreement, *supra*, at 1.

ability to carry out such adverse activities through the foreign storage of call-related information or foreign routing of traffic.[21]

To address these concerns, the Security Agreement includes the following commitments:[22]

- All equipment used to transmit, switch, control, manage or supervise "domestic" communications (calls between points in the United States, including Puerto Rico) must be located in the U.S.;
- All data centers used to provide Internet hosting services for U.S. customers must be located in the U.S.;
- All domestic communications, call records, billing records, and other subscriber information shall be stored exclusively within the U.S. and shall be retained for at least five years;
- All network plans, processes, procedures and other performance information pertaining to the U.S. network shall be maintained in the U.S., but a duplicate copy may be maintained at América Móvil's headquarters in Mexico City;
- All domestic communications shall be routed within the United States, and there shall be no remote access outside the United States to network elements, any capabilities to conduct electronic surveillance and operational support systems, except as agreed to by the U.S. Government;
- TELPRI shall provide to the U.S. Government a comprehensive description of its network, including the locations of servers, routers, switches, operational systems software, and network security appliances and software, and shall provide updates of such description;
- TELPRI shall implement through a reputable third party a screening process for personnel with access to domestic communications facilities, call information or subscriber records, and shall cooperate with any request by the U.S. Government for further screening or to remove any employee;

---

[21] See Department of Homeland Security, *Communications: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Plan* 36 (May 2007) (available at www.dhs.gov/xlibrary/assets/Communications_SSP_5_21_07.pdf) ("Communications Sector Plan"); GAO 2007 Report, *supra*, at 9 ("According to officials from [the Departments of Defense and Justice], [national security] vulnerabilities could result from foreign control of critical infrastructure, such as control of or access to information traveling on networks."); Lewis, *supra*, 57 *Fed. Com. L.J.* at 468-71; The White House, *A National Security Strategy for a New Century* 17 (Dec. 1999) (available at www.dtic.mil/doctrine/jel/other_pubs/nssr99.pdf) ("Our national security and our economic prosperity rest on a foundation of critical infrastructures, including telecommunications.... More than any nation, America is dependent on cyberspace. We know that other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them."); National Strategy, *supra*; Department of Homeland Security, National Infrastructure Protection Plan at 107-21 (2006) (available at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf); Landler & Markoff, "In Estonia, what may be the first war in cyberspace," *Int. Herald Trib*. (May 28, 2007) (available at www.iht.com/bin/print/php?id=5901141).

[22] TELPRI Security Agreement, *supra*, at 7-21.

- If requested by the U.S. Government, TELPRI shall not appoint or shall remove any foreign member of its board or management person at the vice president level or above;
- TELPRI shall appoint not fewer than two directors on its board who are U.S. citizens having security clearances, or eligible to apply for security clearances and approved by the U.S. Government. These "Security Directors" shall serve on a company Security Committee to oversee the company's compliance with this agreement. Each meeting of the board or a board committee must include at least one Security Director;
- TELPRI shall appoint a Head of Security who is a U.S. citizen having, or eligible to apply for, a security clearance. That officer shall submit an annual report to the U.S. Government on the company's compliance with this agreement;
- TELPRI shall not outsource functions covered by this agreement except as agreed to by the U.S. Government; and
- TELPRI shall retain a neutral third party telecom engineer to audit its operations annually, including to develop a security vulnerability and risk assessment.

Unlike some other government procedures leading to agreements with parties to a merger, such as antitrust consent decrees, there is no public report assessing the costs and benefits, competitive impacts or alternatives to the terms of an agreement developed pursuant to CFIUS review.[23] América Móvil has not disclosed its expected costs of complying with these conditions. When Global Crossing was required by CFIUS to implement many of the same conditions, it disclosed that its incremental costs related to information storage, network operations, personnel screening, et cetera, would be approximately $6.5 million in the first year and $2.5 million in each subsequent year.[24]

---

[23] See Tunney Act (applicable to negotiated antitrust consent decrees), 15 U.S.C. §16(e); *United States v. SBC Communications, Inc. and AT&T Corp.*, Case 1:05-CV-02102-EGS (D.D.C. Mar. 29, 2007); United States v. Microsoft Corp., 56 F.3d 1448, 1458-62 (D.C. Cir. 1995); *United States v. AT&T Corp.*, 552 F. Supp. 131, 151 (D.D.C. 1982), aff'd sub nom. Maryland v. United States, 460 U.S. 1001 (1983) ("Divestiture"). See also Office of Management and Budget, Office of Information and Regulatory Affairs, *2006 Report to Congress on the Costs and Benefits of Federal Regulations and Unfunded Mandates on State, Local, and Tribal Entities* (2006); Ellig, "Costs and Consequences of Federal Telecommunications Regulations," 58 *Fed. Com. L.J.* 37 (2006); R. Hahn & R. Litan, Improving Regulatory Accountability (1997) (available at www.aei-brookings.org/admin/authorpdfs/page.php?id=202); K. Arrow, *et al.*, *Benefit-Cost Analysis in Environmental, Health and Safety Regulation* (1996) (available at www.aei-brookings.org/publications/abstract.php?pid=53); Verizon/AM Order, *supra*, at para. 72 (FCC accords deference to Executive Branch expertise on national security and law enforcement issues).

[24] Global Crossing Ltd. 2002 Form 10-K at 10 (filed with the SEC on Dec. 8, 2003) ("While our operations were already generally consistent with the requirements of the Network Security Agreement, we have initiated a number of operational improvements in order to ensure full compliance with the Network Security Agreement. These improvements relate to information storage and management, traffic routing and management, physical, logical, and network security arrangements, personnel screening and training, and other matters. Implementation of and compliance with the Network Security Agreement will require significant upfront and ongoing capital and operating expenditures that are incremental to the Company's historical levels of such expenditures. We estimate that these incremental expenditures will be approximately $6.5 million in 2004 and approximately $2.5 million in subsequent years; however,

2.1.3 Analysis of the TELPRI Security Agreement

The conditions in the Security Agreement are inconsistent with at least four policies in the Communications Act of 1934, as amended (hereafter referred to as "Communications Act") and FCC orders.

2.1.3.1 Unregulated, Widely Available Internet Services

The Telecommunications Act of 1996 includes a strong policy statement against government regulation of Internet services and Internet services providers:[25]

> It is the policy of the United States (1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulations….

Another section of this legislation directs the FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[26] Pursuant to these statutory directions, the FCC in 2005 adopted four policy principles, including promoting competition among Internet network and service providers: "To encourage broadband deployment and to encourage and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers."[27]

Addressing the cross-border nature of the Internet, Congress in the Internet Tax Freedom Act of 1998 directed the President to "seek bilateral, regional, and multilateral agreements to remove barriers to global electronic commerce...."[28] Specifically, Congress declared international negotiating objectives to assure that global electronic commerce is free from tariff and nontariff burdens, as well as burdensome and discriminatory regulation and standards; to accelerate the growth of global electronic commerce, the President should negotiate to expand market access opportunities for the development of telecommunications

---

the actual costs could significantly exceed these estimates.").

[25] 47 U.S.C. § 230(b). See also Vonage Holdings Corp., 19 FCC Rcd 22404, at 22416 (2004) ("long-standing national policy of nonregulation of information services…[allowing providers of information services to] burgeon and flourish in an environment of free give-and-take of the marketplace without the need for and possible burden of rules, regulations and licensing requirements").

[26] § 706(b) of the Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996) (1996 Act), reproduced in the notes under 47 U.S.C. § 157. See also 47 U.S.C. §157(a): "It shall be the policy of the United States to encourage the provision of new technologies and services to the public."

[27] *Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities*, 20 FCC Rcd 14986, at 14988 (2005) ("Internet Policy").

[28] Title XI of P.L. 105-277, the Omnibus Appropriations Act of 1998, Section 1203(a).

infrastructure, procurement of telecommunications equipment, provision of Internet access and telecommunications services, and exchange of goods, services and digitalized information.[29]

In contrast, the Security Agreement imposes various restrictions on TELPRI's Internet services. Its Internet hosting services for U.S. customers must use servers and related services located in the United States Its handling of Internet traffic between two points in the United States must solely use facilities in the United States, and it must provide to the U.S. government descriptions of its facilities. It must manage in the United States its network used to transmit Internet traffic originating or terminating in the United States Additionally, it must not store outside of the United States its customer and traffic records for Internet services provided to U.S. customers.[30]

These conditions comprise federal government regulations that may be detrimental to TELPRI's ability to provide advanced, cost-effective Internet services for U.S. customers. In particular, América Móvil and its affiliates provide extensive Internet hosting, electronic commerce, transmission and other services in Mexico and other countries in the Americas.[31] There are likely to be potential economies of scale and scope regarding servers used in Internet hosting, Internet transmission facilities, managing Internet traffic, and related services.[32] Furthermore, these conditions are not generally applicable to providers of Internet services in the United States, including those that TELPRI competes against.

---

[29] *Id.* at Section 1203(b).

[30] In connection with a CFIUS review, in January 2007 Global Crossing agreed to similar restrictions on one foreign-owned provider's hosting services and data centers. Petition to Adopt Conditions to Authorizations and Licenses filed by the Department of Justice, Federal Bureau or Investigation and Department of Homeland Security, WC Dkt. No. 06-215 (filed Feb. 1, 2007) (available at svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518724528 and svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518724527). The FCC approved the merger subject to Global Crossing abiding by these commitments. FCC Public Notice, *Domestic 214 Authorization Granted: Application Filed for the Transfer of Control of Impsat USA, Inc. from Impsat Fiber Networks, Inc. to Global Crossing Limited*, DA 07-606 (Feb. 8, 2007). Such restrictions on one provider's Internet services and facilities were not in the CFIUS agreement with Global Crossing in September 2003. Global Crossing, 18 FCC Rcd 20301, at Appendix D (2003).

[31] América Móvil 2005 Form 20-F at 22; Telefonos de Mexico, S.A. de C.V. 2005 Form 20-F at 19, 37, 38 (filed with the SEC on June 29, 2006).

[32] See "Telmex will offer integrated services of 'hosting' in seven countries" (Nov. 14, 2006) (available at http://66.218.71.231/language/translation/translatedPage.php?lp=es_en&text=http%3a%2f%2fwww.terra.com%2fnoticias%2farticulo%2fhtml%2fact647858.htm#); S. Mehta, "Behold the server farm," *Fortune* (July 28, 2006) (available at http://money.cnn.com/2006/07/26/magazines/fortune/futureoftech_serverfarm.fortune/index.htm); "Servers as High as an Elephant's Eye," *Business Week* (June 12, 2006) (available at www.businessweek.com/magazine/content/06_24/b3988087.htm).

2.1.3.2 Deregulation of Carriers' Facilities and Service Offerings

In the era of monopolistic telecommunications carriers, the FCC required carriers to obtain prior approval for the addition or termination of lines and service offerings.[33] With the growth of competition, the FCC found that such regulations were not necessary to protect the public interest; on the contrary, such regulations impaired the carriers' ability to satisfy customers' needs, efficiency and competition.[34] Accordingly, the FCC gave carriers freedom to make decisions on network facilities, network operations and service offerings without government review or restrictions.

The Security Agreement takes a conflicting approach by restricting the locations of TELPRI's lines, switches and network management centers, as well as how TELPRI routes traffic. While the carrier can add lines without prior approval by the U.S. government, all lines used to transmit domestic traffic must be located in the United States The Security Agreement bars the likely potential to reduce costs by utilizing network operating centers, lines or switches outside of the United States Such restrictions can impair the efficiency of the carrier's operations and its ability to deploy advanced services.

2.1.3.3 Fostering Economies from Mergers

In determining whether a proposed merger will advance the public interest, the FCC often relies on the benefits of likely economies of scale, scope and vertical integration resulting from the merger.[35] Such economies can yield various public benefits including lower prices to users, increased ability to invest in infrastructure upgrades, greater capability to deploy advanced services, more competition, and increased reliability of services. In fact, the FCC has found that such economies resulting from mergers promote national security.[36] Unless there are offsetting concerns about anticompetitive conduct or other harms, the FCC generally allows merging carriers to integrate their operations and capture the economies of scale and scope.

The Security Agreement imposes a range of restrictions on América Móvil's ability to integrate TELPRI with its other operations in the Americas. The restrictions cover TELPRI's network, network operating centers and network planning; data processing and storage equipment

---

[33] See 47 U.S.C. §214; Long-Run Regulation of AT&T's Basic Domestic Interstate Services, 95 F.C.C. 2d 510, 521-23 (1983).

[34] See *Policy and Rules Concerning the Interstate, Interexchange Marketplace*, 11 FCC Rcd 20730 (1996); *Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefor*, Fourth Report and Order, 95 F.C.C. 2d 554 (1983), *vacated sub nom. Am. Tel. & Tel. Co. v. FCC*, 978 F.2d 727 (D.C. Cir. 1992).

[35] See *Verizon Communications Inc. and MCI, Inc.: Applications for Approval of Transfer of Control*, 20 FCC Rcd 18433, at paras. 202-07 (2005) ("Verizon/MCI").

[36] *Id.* at paras. 197-201.

and operations; and billing and other customer services. The loss of economies of scale and scope could lessen the public benefits ordinarily associated with such a merger.

2.1.3.4 Decreasing Regulatory Burdens on Service Providers

Finally, Congress has directed the FCC to review its regulations and eliminate regulatory burdens which are no longer necessary in the public interest.[37] Congress determined that reducing regulatory burdens on telecom carriers will serve the public interest by decreasing costs and delays for services. Accordingly, the FCC has reduced various regulatory requirements, including by streamlining license applications, eliminating tariff filings for most carriers, adjusting and limiting accounting standards, reducing rate regulations, cutting reporting requirements, and decreasing service unbundling requirements.[38]

In contrast, the Security Agreement implements new regulatory burdens on one foreign-owned carrier.[39] These burdens include personnel screening, annual security audits, information storage requirements and restrictions, and reporting requirements.

An argument could be made that the national-security rationale for some of these restrictions, such as personnel screening, would apply to a larger set of carriers than those subject to recent foreign acquisitions. The FCC has responsibilities for promoting national defense and safety,[40] and it has broad statutory authority to adopt regulations, or impose conditions on licenses

---

[37] 47 U.S.C. §§160, 161.

[38] See, e.g., *Unbundled Access to Network Elements*, 20 FCC Rcd 2533 (2005) ("Unbundled Access"), *aff'd sub nom. Covad Communications Co. v. FCC*, 450 F.3d 528 (DC Cir. 2006); F*ederal-State Joint Conference on Accounting Issues*, 19 FCC Rcd 11732 (2004); *Implementation of Further Streamlining Measures for Domestic Section 214 Authorizations*, 17 FCC Rcd 5517 (2002).

[39] The Security Agreement includes conditions not imposed in the earlier CFIUS agreements with Deutsche Telekom in the VoiceStream Wireless transaction, *Applications of VoiceStream Wireless Corp., PowerTel, Inc., Transferors, and Deutsche Telekom AG, Transferee*, 16 FCC Rcd 9779 (2001) ("DT"), or with Telmex in its proposed transaction with XO Communications (available at gullfoss2.fcc.gov/prod/eefs/retrieve.cgi?native_or_pdf&id_document=6513291830). See also note 23 to this chapter.

[40] See 47 U.S.C. §§151 (purpose of FCC regulations includes national defense and promoting safety of life and property), 214(c) (FCC may attach to the issuance of a certificate to acquire or operate lines "such terms and conditions as in its judgment the public convenience and necessity may require"), 219 (FCC may require annual reports from all carriers), 220 (FCC may prescribe the forms for all records to be kept by carriers and FCC shall at all times have access to all documents kept or required to be kept by carriers), 301 (conditions for radio licenses) and 303(r) (restrictions and conditions for radio licenses).

See descriptions of some of the FCC's post-9/11 actions to promote national defense and public safety in: Testimony of K. Moran (Director, Office of Homeland Security, Enforcement Bureau, FCC) Before the U.S. House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, "CyberSecurity: Protecting America's Critical Infrastructure, Economy & Consumers" (Sept. 13, 2006) (available at www.fcc.gov/ola/docs/moran091306.pdf); Statement of K. Martin (Chairman, FCC) Before the U.S. House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, "Hearing on Public Safety Communications from 9/11 to Katrina: Critical Public Policy Lessons" (Sept. 29, 2005) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261417A1.pdf); Statement of J. Dailey (Director, Office of

and authorizations, for telecom carriers.[41] The FCC could make some of the conditions in the Security Agreement, or similar requirements, to promote national security applicable industry-wide or for a category of carriers.

To date, in the context of the long-standing policy of reducing unnecessary regulatory burdens, the FCC has not found that the public interest would be served by imposing these new regulatory burdens on all domestic or foreign-owned carriers. Moreover, neither the Communications Sector Security Plan adopted by the Department of Homeland Security and other signatory agencies, nor the best practices recommendations of an FCC advisory group, has taken an industry-wide approach to these safeguards.[42]

2.2 Restrictions on Globalization of Operations for a Telecom Equipment Provider to Promote U.S. National Security

2.2.1 Background on the Alcatel/Lucent Transaction

On November 30, 2006, Alcatel and Lucent closed a "merger of equals" to create a leading global communications solutions provider.[43] The merged company is named Alcatel-Lucent and is headquartered in Paris. Post-merger, Alcatel-Lucent had a presence in 130 countries and about 79,000 employees, of which approximately 23,000 were engaged in research and development.

Lucent was the corporate successor to Western Electric Company, Inc., the telecom equipment research, development, manufacturing and supply arm of the monopoly Bell System

---

Homeland Security, Enforcement Bureau, FCC) Before the U.S. House Select Committee on Homeland Security, Subcommittee on Emergency Preparedness and Response, "The Emergency Alert System (EAS)" (Sept. 22, 2004) (available at www.fcc.gov/homeland/documents/dailey092204.pdf).

[41] See *Atlantic Tel-Network, Inc. v. FCC*, 59 F.3d 1384, 1389 (DC Cir. 1995) (FCC could impose condition on license even if no such formal policy existed when the condition was imposed); FCC v. National Citizens Committee for Broadcasting, 436 U.S. 775 (1978); U*nited States v. Southwestern Cable Co*., 392 U.S. 157, 177-78 (1968) (FCC's ancillary jurisdiction); *United States v. Midwest Video Corp*., 406 U.S. 649 (1972) (same); *Applications for the Assignment of License from Denali PCS, L.L.C. to Alaska DigiTel, L.L.C. and the Transfer of Control of Interests in Alaska DigiTel, L.L.C. to General Communication, Inc*., FCC 06-185, at Appendix A (2006) (adopting conditions restricting access to business records and other information). See generally Tramont, "Too Much Power, Too Little Restraint: How the FCC Expands its Reach Through Unenforceable and Unwieldy 'Voluntary' Agreements," 53 *Fed. Com. L.J*. 49 (2000).

[42] See Section 5.3 of this report.

[43] Alcatel-Lucent Press Release, "Alcatel and Lucent complete merger creating world's leading communication solutions provider" (Nov. 30, 2006) (available at www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3cQ7SL8h2VAQAu32oaA!!?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=News_Releases_2006/News_Article_000012); Alcatel/Lucent Announcement, *supra*. This transaction to increase the global strength of two leading telecom equipment manufacturers was announced the day before América Móvil announced its regional geographic expansion through an agreement to acquire three Caribbean telecom service providers.

before January 1, 1984.[44] Pursuant to an antitrust consent decree, the Bell Operating Companies (local exchange carriers) were divested from AT&T Company; Western Electric remained with AT&T until it was spun-off to shareholders in 1996 under the Lucent name.[45] Lucent also owned Bell Laboratories, which was a leading telecom research and development organization based in New Jersey. With operations in the United States and several foreign countries, Bell Labs performed work for Lucent's commercial products as well as projects for the U.S. government.[46]

The telecom equipment industry and Lucent changed dramatically since the days of Western Electric's role in the vertically integrated, monopoly Bell System. In the earlier era (1976), Western Electric operated twenty-three major plants scattered around the United States and focused on supplying the domestic operations of the Bell System.[47] Through regulatory and antitrust decisions as well as other market developments, the industry and Lucent became global.[48] Several foreign-owned telecom equipment manufacturers became major suppliers to U.S. service providers and customers. Similarly, U.S. manufacturers sold in the expanding foreign markets. Moreover, even when U.S.-owned manufacturers sold to U.S. customers, many of their products relied on foreign operations or foreign suppliers for research and development, manufacturing and support services.[49]

Prior to the merger, each of Alcatel and Lucent was operating in the United States as well as globally.[50] Neither company provided telecom or Internet services in the United States Instead,

---

[44] Alcatel-Lucent, "A brief history of Lucent Technologies" (available at http://www.bell-labs.com/history/lucent.html).

[45] *Id.*; Divestiture, *supra*. After Lucent's separation from AT&T, Lucent spun off its enterprise networking group (Avaya Inc.) in 2000 and separated (through an initial public offering) its microelectronics business (Agere Systems) in 2001.

[46] Alcatel-Lucent, "Research Areas & Projects" (available at www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3MXMBSYGYRq6m-pEoYgbxjggRX4_83FT9IH1v_QD9gtzQiHJHR0UAaOmbyQ!!/delta/base64xml/L3dJdyEvd0ZNQUFzQUMvNElVRS82X0FfNFA2); Alcatel-Lucent, "Global Labs" (available at www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3MQ7UL8h2VAQAPt9UAg!!).

[47] J. Brooks, *Telephone: The First Hundred Years* at 12 (1976); A. von Auw, *Heritage & Destiny: Reflections on the Bell System in Transition* at 200-08 (1983) ("von Auw"); Hausman, "The Bell Operating Companies and AT&T Venture Abroad While British Telecom and Others Come to the United States," in S. Bradley, et al., *Globalization, Technology and Competition* at 313, 314 (1993).

[48] AT&T (Docket No. 19129, Phase II), 64 F.C.C. 2d 1, 26-45 (1977) ("FCC Docket 19129") ; Divestiture, *supra*; von Auw, *supra*, at 200-08; Lucent Technologies Inc., Form S-1/A (filed with the SEC on Apr. 1, 1996) (discussion of competition and markets).

[49] See Lucent Technologies Inc. 2005 Form 10-K at 6 (filed with the SEC on Dec. 14, 2005) ("Lucent 2005 Form 10-K"); International Telecommunication Union, W*orld Telecommunication Development Report 1996/97: Trade in Telecommunications* (1998); OECD, T*elecommunications Equipment: Changing Markets and Trade Structures* (1991) (available at www.oecd.org/dataoecd/56/54/1909439.pdf).

[50] Lucent 2005 Form 10-K at 17 ("We are a global company. Our foreign operations include integration, manufacturing and test facilities, engineering centers, sales personnel and customer support functions. For fiscal 2005

each company sold products to telecom carriers, Internet services providers, enterprise customers and other end-users. Each company's U.S. sales involved some products which were, in large part, developed, manufactured and supported in the United States Also, each company's U.S. sales involved some products which were, in large part, developed, manufactured and supported by its operations outside of the United States As global suppliers, each company also sold some products outside the United States which were, in large part, developed, manufactured and supported by its operations in the United States

In announcing the merger, the companies pointed to "a strategic fit between two experienced and well-respected global communications leaders who together will become the global leader in convergence" for next-generation networks.[51] The companies expected the merger to produce about $1.7 billion in annual cost synergies.[52]

2.2.2 Security Agreements for the Alcatel/Lucent Transaction

On November 17, 2006, President George W. Bush accepted the recommendation of CFIUS that he not suspend or prohibit the Alcatel/Lucent transaction, provided that the companies execute a certain National Security Agreement and a certain Special Security Agreement.[53] The White House release calls these conditions "robust and far-reaching agreements designed to ensure the protection of our national security."

Like most conditions accepted by companies in order to terminate a CFIUS review or investigation, the terms of these agreements were not made public. Nor is there much public

---

and 2004, we derived approximately 37% and 39%, respectively, of our revenues from sales outside the U.S., including in China, Europe, India and various countries in the Middle East, such as Iraq and Israel. We are committed to expanding our business outside the U.S."); Alcatel 2004 Form 20-F at 20 (filed with the SEC on Mar. 31, 2005) ("We have administrative, production, manufacturing and research and development facilities worldwide. A substantial portion of our production and research activities in all business areas is conducted in France and China. We also have operating affiliates and production plants in many other countries, including Germany, Italy, Spain, Belgium, Denmark, the United Kingdom, Canada, the United States and Mexico.").

[51] Alcatel/Lucent Announcement, *supra*, at 2.

[52] *Id.* at 3.

[53] The White House Release, "Statement on CFIUS Recommendation Regarding Proposed Merger of Lucent Technologies, Inc., and Alcatel" (Nov. 17, 2006) (available at www.whitehouse.gov/news/releases/2006/11/20061117-13.html) ("White House Release"). See also S. Kirchgaessner, "Washington slaps review on Nokia-Siemens venture" (Jan. 7, 2007) (available at www.ft.com/cms/s/e07c2be8-9e86-11db-ac03-0000779e2340.html). The Special Security Agreement addresses classified and other work for the federal government. See Lucent Technologies Inc. Form 8-K (filed with the SEC on Nov. 17, 2006) ("Lucent 8-K"); Alcatel-Lucent Press Release, "Alcatel-Lucent announces independent subsidiary to serve the U.S. federal government market" (Dec. 1, 2006) (available at www.lgsinnovations.com/wps/portal/lgs/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKL94x3dgzWL8h2VAQASmcpgQ!!?LMSG_CABINET=LGS&LMSG_CONTENT_FILE=Press_Releases_2006/LGS_News_Article_000001.xml); Defense Security Service, Special Security Agreement (available at www.dss.mil/isec/SpecialSecurityAgreement.pdf); Section 5.2, *infra*.

information on the national security concerns identified by CFIUS with regard to this transaction. Clearly, this secrecy impairs the following analysis.

Nevertheless, one piece of public information about this National Security Agreement points to what appear to be inconsistencies or conflicts with several communications policies in order to address national security concerns. In a filing with the Securities and Exchange Commission, Lucent said that this agreement "provides for certain undertakings with respect to the U.S. businesses of Lucent and Alcatel relating to the work done by Bell Labs and *to the communications infrastructure in the United States*."[54] In other words, Alcatel and Lucent agreed to some conditions not generally applicable through U.S. laws and regulations affecting their supply of products to U.S. carriers and other customers. This statement also indicates that the National Security Agreement addresses operations going beyond Lucent's classified and other work for the U.S. government, to supplying the communications infrastructure of commercial carriers. The filing goes on to state: "The provisions contained in both the National Security Agreement and the Special Security Agreement are not expected to impact the projected synergies to be realized from the merger transaction or materially impact the integration of the businesses."[55]

2.2.3 Analysis of the Alcatel/Lucent National Security Agreement

Even from the small public indication of the conditions in this National Security Agreement, there appear to be at least four telecommunications industry policies which may conflict with, or point in a different direction than, these conditions.

2.2.3.1 Freedom to Interconnect Equipment that Does Not Cause Technical Harm to Telecom Networks

Before 1968, the Bell System provided all equipment that could be used in or interconnected to its networks, and did not allow "foreign attachments." The FCC determined that the Bell System applied this approach in an excessively restrictive manner, barring equipment that would do no technical harm to the Bell System's networks and thereby restricting innovation and increasing costs.[56]

Since 1968, the FCC has administered standards and certification procedures designed to allow interconnection of any equipment chosen by the customer or service provider as long as it does not cause technical harm to public telecom networks.[57] The technical standards for terminal

---

[54] Lucent 8-K, *supra* (emphasis added).

[55] *Id.*

[56] Carterfone, 13 F.C.C.2d 420 (1968). See also *United States v. AT&T*, 524 F. Supp. 1336, 1348 (D.D.C. 1981).

[57] 47 CFR Part 68; *2000 Biennial Regulatory Review of Part 68 of the Commission's Rules and Regulations*, 15 FCC Rcd 24,944 (2000), recon., FCC 02-103 (2002) ("Biennial Review"); FCC, "Part 68 Frequently Asked Questions"

equipment cover factors such as electrical emissions and power levels. To facilitate the rapid, low-cost availability of equipment for selection by customers, the FCC adopted procedures allowing testing and certification by manufacturers and accredited third parties (including foreign entities). These standards and procedures apply equally to domestic and foreign-manufactured equipment.

In furtherance of this well-established policy, in 2005 the FCC adopted the following principle pertaining to equipment used in Internet services: "To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to connect their choice of legal devices that do not harm the network." [58]

In addition to promoting competition and innovation in the telecom equipment available to customers in the United States, this emphasis on open markets allows manufacturers to make decisions on how and where to develop, manufacture and support their products. U.S.-owned as well as foreign-owned manufacturers can choose to locate any operation outside the United States or to obtain any component or service from a third party outside the United States, as long as the resulting equipment satisfies the FCC's standards and processes for not causing technical harm to telecom networks.[59]

---

at 1 (available at www.fcc.gov/wcb/iatd/part68faqs.pdf) ("Under Part 68, wireline telecommunications carriers must allow all TE [terminal equipment] to be connected directly to their networks, provided the TE meet certain technical criteria for preventing four prescribed harms. The harms are electrical hazards to operating company personnel, damage to network equipment, malfunction of billing equipment, and degradation of service to customers other than the user of the TE and that person's calling and called parties.").

[58] Internet Policy, *supra*, 20 FCC Rcd at 14988.

[59] See FCC, "Equipment Authorization of Telephone Terminal Equipment" at 2 (June 2006) (available at www.fcc.gov/oet/ea/TCB-part-68-list.pdf) (FCC recognition of Telecommunications Certification Bodies to perform equipment authorizations in Germany, Netherlands, Singapore and United Kingdom); Biennial Review, supra, at 24,947 ("The Part 68 rules are premised on a compromise whereby providers are required to allow terminal equipment manufactured by anyone to be connected to their networks, provided that the terminal equipment has been shown to meet the technical criteria for preventing network harm that are established in the Part 68 rules.... Our rules have facilitated a vibrant, competitive market for terminal equipment, reducing prices and resulting in a proliferation of new equipment and capabilities available to consumers."); Lucent 2005 Form 10-K at 17 ("We are also dependent on international suppliers for some of our components and subassemblies and for assembly of some of our products."); Hookway, "Vietnam Vies to Get In on Outsourcing," *Wall St. J.* (May 29, 2007) A-6 (Vietnamese companies develop software for Nortel Networks Corp. and Alcatel-Lucent).

On the other hand, some in the U.S. federal government are concerned about higher security risks related to use of foreign manufacturing operations for U.S. critical infrastructure. See Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection at 14 (Jan. 2007) ("Some critical [defense industrial base] assets are located overseas. This severely limits the ability of the DoD to use regulatory mechanisms to ensure compliance with security guidelines, although threats to overseas [defense industrial base] assets may be inherently greater and at higher risk than domestic [defense industrial base] assets."). See also National Defense Critical Infrastructure Protection Act of 2006, H.R. 4881, 109th Cong., 2nd Sess. (proposed legislation to ensure that infrastructure critical to national security is controlled by U.S. citizens).

For U.S. manufacturers, the U.S. government has also worked to open foreign markets for terminal and other telecommunications equipment based on transparent international technical standards.[60]

From the small public description of the Alcatel/Lucent National Security Agreement, it is not possible to determine whether the "robust and far-reaching" conditions relating to the communications infrastructure of the United States impose a significant burden on this company's supply of equipment and services for U.S. customers. Perhaps there will be no adverse effects on the prices, timing and features of equipment available to U.S. customers. However, the national security conditions may go beyond the technical-harm standards and processes under the FCC's rules that are generally applicable to U.S. and foreign suppliers of telecom equipment to U.S. customers. Furthermore, such national security conditions would not have been applicable to Lucent, or even to Alcatel's sales in the United States, but for Alcatel's merger with Lucent and the consequential CFIUS review of this transaction.

2.2.3.2 Open Markets for Telecom Equipment Suppliers

The U.S. Trade Representative has objected to restrictions in some countries on imports of U.S.-manufactured telecom equipment.[61] Similarly, the U.S. government encourages competition

---

[60] See Section 2.2.3.1 and Section 4.3 of this report (U.S.-Korea Free Trade Agreement); Irving, "Steps Toward a Global Information Infrastructure", 47 *Fed. Com. L.J.* 271, at 277 (1994) (former Assistant Secretary, U.S. Department of Commerce) ("Today, the international arena is beset with a multiplicity of different technical standards, formats, and requirements that make interconnection and interoperability, and therefore communications, very difficult. One of the administration's goals is to continue our active participation in international standard-setting activities and encourage other countries to ensure that interoperability of networks-among countries, networks, and individual users and information providers-is afforded the highest priority. The United States has played a leadership role in the international standardization process developed through the ITU, the International Electrotechnical Commission, and the International Organization for Standardization. It also has illustrated its commitment to global telecommunications standardization through the establishment of Committee T1, which develops national telecommunications network standards for the United States and drafts and proposes U.S. technical contributions to the ITU.").

[61] See United States Trade Representative, "USTR Issues 2005 '1377' Review of Telecommunications Trade Agreements; Renewed Focus on Identifying, Dismantling Telecommunications Trade Barriers Around the World" (Mar. 31, 2005) (available at www.ustr.gov/Document_Library/Press_Releases/2005/March/USTR_Issues_2005_1377_Review_of_Telecommunications_Trade_Agreements.html) (concerns about burdensome testing and certification requirements in Mexico and Korea, and limitations on suppliers' choice of technology in China and Korea); United States Trade Representative, "U.S. and Korea Resolve Major Trade Dispute in Telecom Sector" (Apr. 23, 2004) (available at www.ustr.gov/Document_Library/Press_Releases/2004/April/US_Korea_Resolve_Major_Trade_Dispute_in_Telecom_Sector.html) (under pressure from the U.S., Korea agrees not to adopt a technical standard for wireless systems that would have shut out systems from U.S. manufacturers); United States Trade Representative, "U.S. and EU Implement Agreement to Reduce Barriers on Transatlantic Trade of Telecommunications and Electronics Products" (Jan. 17, 2001) (available at www.ustr.gov/Document_Library/Press_Releases/2001/January/US_EU_Implement_Agreement_to_Reduce_Barriers_on_Transatlantic_Trade_of_Telecommunications_Electronics_Products.html) (reducing barriers to approximately $30 billion in annual transatlantic trade of telecommunications and electronics products by eliminating duplicative product testing requirements); Section 4.3 of this report.

among telecom equipment manufacturers (without limiting foreign corporations or foreign-sourced products) and generally allows manufacturers to make market decisions on technologies, manufacturing operations, investments and locations. Instead of regulations, the U.S. government generally relies on market forces to promote the availability of telecom equipment with advanced features, low prices and capabilities which meet customers' needs.

There are a few areas of industry-wide FCC regulations requiring equipment to comply with certain performance standards and capabilities in furtherance of national security in terms of law enforcement activities and emergency services.[62] Furthermore, telecom equipment manufacturers have participated in promoting the security of telecom and Internet networks through government-sponsored efforts (such as the National Security Telecommunications Advisory Committee and the Network Reliability and Interoperability Council)[63] as well as industry committees and efforts at individual companies. These regulations and national security efforts have not differentiated between U.S. and foreign ownership or operations of manufacturers.

The undertakings to protect the communications infrastructure of the United States in the National Security Agreement have not been disclosed. If they involve restrictions on the operations and business decisions of this foreign-incorporated telecom equipment manufacturer, then these conditions would go in a different direction than the open-borders, deregulated, free-market approach of the U.S. Trade Representative and FCC.

2.2.3.3 Deregulation of Carriers' Decisions on the Selection and Deployment of Equipment

The FCC and state regulators used to play a significant role in approving carriers' capital expenditures for facilities, and in some cases the selection and deployment of equipment used in carriers' networks. As noted above, the FCC required prior approval for the addition or termination of interstate lines by carriers.[64] Such regulations were replaced by blanket authorizations, allowing carriers to make independent, market-driven decisions on what equipment to deploy, where, with what features and capacity, and from what suppliers. [65]

---

[62] See Section 2.2.3.1 of this report.

[63] See National Security Telecommunications Advisory Committee (NSTAC) (available at www.ncs.gov/nstac/nstac.html); NSTAC, *Issue Review: A Review of Issues Addressed Through NSTAC XXIX* (Aug. 2006) (available at http://www.ncs.gov/nstac/reports/2006/NSTAC%20XXIX%20Issue%20Review.pdf); NSTAC, *Globalization Task Force Report* (May 2000) (available at http://www.ncs.gov/nstac/reports/2000/GTF-Final.pdf); The Network Reliability and Interoperability Council (available at http://www.nric.org/).

[64] See notes 44-45, *supra*.

[65] Along these lines, the FCC removed unbundling regulations applicable to new network facilities so as to encourage carriers to make market-based decisions on equipment deployments and technologies. Unbundled Access, *supra*.

Furthermore, the FCC and state regulators used to engage in rate regulation based on the carriers' costs, including whether to allow a carrier to recover capital expenditures for certain network equipment. Such regulations were replaced by price caps or other alternative approach for carriers with market power (by which rates are not based on carriers' actual costs and regulators do not determine whether to disallow certain capital expenditures), and deregulation of rates charged by nondominant (competitive) carriers.[66] As an additional check on equipment purchases in an earlier era, regulators required prior approval for new service offerings; this constrained carriers' investments in some equipment with capabilities to support new features. Again, regulators have decreased reviews of new services and have encouraged carriers to deploy equipment with advanced features of their choice.[67]

There are a few areas in the communications laws and regulations which impose requirements on carriers' equipment. For example, a statute and FCC rules require carriers to implement equipment with specified capabilities to assist law enforcement activities (such as wiretapping), and telecom equipment manufacturers shall make available to carriers such equipment at reasonable charges.[68] Also, the FCC has adopted rules for carriers to deploy equipment providing connection to, and automatic location of users by, emergency services.[69] These requirements are applicable industry-wide, to domestic as well as foreign-sourced equipment, regardless of whether the manufacturer is U.S.-owned or foreign-owned.

It is not possible to determine from public information how and to what extent the National Security Agreement affects the availability of options for U.S. carriers' decisions on the selection and deployment of equipment. In at least some ways, the U.S. government has increased its influence over a leading provider's costs, features, supply or support for equipment. This affects the equipment that carriers can select and deploy. Moreover, unlike the requirements for law

---

[66] See *Policy and Rules Concerning Rates for Dominant Carriers*, 4 FCC Rcd 2873 (1989); AT&T Reclassification Order, 11 FCC Rcd 3271 (1995); *Motion of AT&T to be Declared Non-Dominant for International Service*, 11 FCC Rcd 17,963 (1996).

[67] See 47 U.S.C. §157(a) ("It shall be the policy of the United States to encourage the provision of new technologies and services to the public."); notes 36 and 70, *supra*; Lavey, "Innovative Telecommunications Services and the Benefit of the Doubt," 27 *Cal. W. L. Rev.* 51 (1990).

[68] Communications Assistance for Law Enforcement Act ("CALEA"), P.L. No. 103-414, 108 Stat. 4279 (1994); 47 U.S.C. §1002 (obligations of telecommunications carriers with regard to law enforcement assistance capabilities of its equipment, facilities and services); 47 U.S.C. §1005(b) ("a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements of section 1002").

[69] *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 18 FCC Rcd 25,340 (2003); *IP-Enabled Services and 911 Requirements for IP-Enabled Service Providers*, 20 FCC Rcd 10,245 (2005).

enforcement and emergency services capabilities, the conditions in the National Security Agreement only apply to equipment from one foreign-owned supplier.

2.2.3.4 Nondiscrimination among Telecom Equipment Manufacturers

In addition to the regulatory/antitrust attack on the Bell System's equipment interconnection restrictions, the United States developed a strong regulatory and antitrust policy against the Bell System's practices of excluding unaffiliated manufacturers from the carriers' procurements of network equipment. The FCC's order in 1977 prohibited this discriminatory exclusion of competing telecom equipment manufacturers.[70] Later, the antitrust consent decree that broke up the Bell System reflected on-going concerns about discrimination in telecom equipment procurements by barring the Bell Operating Companies from engaging in manufacturing and from discriminating among manufacturers.[71]

When Congress lifted the restriction on the Bell Operating Companies' entry into manufacturing in 1996, the statute continued the policy of nondiscrimination in carriers' equipment procurements through several safeguards.[72] The protections apply industry-wide, without regard to the manufacturer's country of incorporation or the equipment's place of origin.

The National Security Agreement takes a different approach. Through CFIUS's review of a single foreign acquisition, national security conditions are made to apply solely to one manufacturer. Other foreign-incorporated manufacturers (unless covered by similar agreements following CFIUS reviews of their acquisitions of U.S. businesses), the foreign-sourced equipment of domestic or other foreign manufacturers, and the U.S.-sourced equipment of domestic or other foreign manufacturers are not covered by such conditions. While these conditions do not prohibit carriers from procuring equipment from a leading foreign provider, they are at odds with the policy of nondiscrimination among telecom equipment manufacturers in the actions of Congress, the FCC and the Antitrust Division of the Justice Department.

---

[70] *FCC Docket 19129, supra; Consolidated Application of American Telephone and Telegraph Company and Specified Bell System Companies for Authorization Under Sections 214 and 310(d)*, 96 F.C.C.2d 18, at 58-59 (1983) ("We have always believed that increased competition should facilitate operating company purchase of the most cost effective equipment available and accelerate the introduction of new service features.").

[71] Divestiture, *supra*, 552 F. Supp. at 190-91. See Lavey & Carlton, "Economic Goals and Remedies of the AT&T Modified Final Judgment," 71 *Geo. L.J.* 1467 (1983).

[72] 47 U.S.C. §§272, 273.

Chapter Three

FCC Conditions on a Merger of Domestic Telecom Carriers

The FCC's order approving the largest domestic telecom merger accepted a commitment against using offshore labor and failed to impose the national security burdens which it adopted for foreign acquisitions.

3.1 Background on the AT&T/BellSouth Transaction

On March 5, 2006, AT&T and BellSouth announced their agreement to merge. The domestic companies were leading wireline carriers and joint owners of the large wireless carrier Cingular. Among the claims of merger benefits, the companies pointed to expected net present value of $18 billion in synergies; creating a more innovative and efficient carrier operating a single fully integrated wireless and wireline Internet Protocol network offering a full range of advanced solutions; and giving "business and government customers, including military and national security agencies, a reliable U.S.-based provider of integrated, secure, high-quality and competitively priced services to meet their needs anywhere in the world."[1] The expected synergies included cutting about 10,000 jobs.[2]

Because the transaction did not involve a foreign acquirer, there was no CFIUS review. The Antitrust Department of the Justice Department closed its investigation of the transaction on October 11, 2006 without requiring divestitures or imposing any condition.[3]

In contrast, the FCC struggled to reach an order accepted by a majority of the commissioners. With one commissioner recused,[4] the two Democratic commissioners diverged from the Republican chairman and other Republican commissioner. The Democratic commissioners sought a range of conditions, many similar to what AT&T had accepted in 2005 in connection with the merger of AT&T and SBC (also reflected in conditions to approval of the

---

[1] AT&T and BellSouth Press Release, "AT&T, BellSouth to Merge; Combination Will Speed Innovation, Competition and Convergence" (Mar. 5, 2006) (available at www.sec.gov/Archives/edgar/data/732713/000095012306002637/y18291e425.htm).

[2] See AT&T Inc. and BellSouth Corporation, "AT&T, BellSouth Merger: Substantial Synergy Opportunities, Strengthened Growth Platforms in Wireless, Business and Integrated Services" at 36 (Mar. 5, 2006) (available at www.sec.gov/Archives/edgar/data/732713/000095012306002593/y18291se425.htm).

[3] The Justice Department concluded that the transaction was not likely to reduce competition substantially, and would likely result in cost savings and other efficiencies that should benefit consumers. Department of Justice Press Release, "Statement by Assistant Attorney General Thomas O. Barnett Regarding the Closing of the Investigation of AT&T's Acquisition of BellSouth; Investigation Concludes that Combination Would Not Reduce Competition" (Oct. 11, 2006) (available at www.justice.gov/atr/public/press_releases/2006/218904.htm).

[4] Statement of Commissioner Robert M. McDowell Re Application for Transfer of Control of AT&T Inc. and BellSouth Corporation (Dec. 18, 2006) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-269058A1.pdf).

merger of Verizon and MCI on the same day).[5] The 2005 conditions included commitments on rate freezes for special access services, offerings of unbundled network elements, broadband deployment, Internet backbone interconnections, and compliance with the FCC's Internet neutrality policy principles. Notably, the 2005 conditions did not include job repatriation or other national security/anti-globalization commitments.

There were several attempts by FCC Chairman Kevin Martin over almost three months to bring an order to a vote for the AT&T/BellSouth transaction.[6] After being unable to obtain a majority to support approval of the transaction without conditions, the FCC received an offer of conditions by the merging parties on October 13, 2006; this offer was then subject to public comments as well as numerous meetings for interested parties with the commissioners and staff.[7] After describing the offered conditions (regarding broadband services, public safety and disaster recovery, unbundled network elements, special access, wireless, transit service and Internet neutrality), the companies noted in the offer: "we also discussed the possibility of further conditions relating to the repatriation to the BellSouth territory of jobs that had been expatriated to overseas locations."[8] Finally, the companies filed a revised offer of conditions on December 28, 2006.[9] The FCC voted on December 29, 2006 to approve the transaction subject to the offered conditions,[10] and the companies closed the merger that day.[11]

Two other pieces of background information on this transaction are helpful. First, the U.S. government was aware that the U.S. telecommunications industry lost hundreds of thousands of jobs since its peak around March 2001.[12] The most prominent factors appear to be unrelated to

---

[5] *SBC Communications Inc. and AT&T Corp.: Applications for Approval of Transfer of Control*, 20 FCC Rcd 18290, Appendix F (2005) ("SBC/AT&T); Verizon/MCI, *supra*, at Appendix G.

[6] FCC Release, "Deletion of Agenda Items from October 12, 2006, Open Meeting and FCC to Hold an Additional Open Meeting, Friday, October 13, 2006, at 11:00 a.m." (Oct. 11, 2006); FCC Release, "Open Commission Meeting Scheduled for October 13, 2006, Cancelled" (Oct. 13, 2006); Commissioners Michael Copps and Jonathan Adelstein, "Letter Concerning the AT&T/BellSouth Merger" (Oct. 13, 2006); Chairman Kevin Martin, "Next Steps for Review of AT&T/BellSouth Transfer of Control Application" (Oct. 13, 2006); FCC Release, "Deletion of Agenda Item from November 3, 2006, Open Meeting" (Nov. 2, 2006).

[7] FCC Public Notice, "Application for Approval of Transfer of Control Filed by AT&T Inc. and BellSouth Corporation; Commission Seeks Comment on Proposals Submitted by AT&T Inc. and BellSouth Corporation," DA 06-2035 (Oct. 13, 2006).

[8] *Id.*, Attachment at 6.

[9] AT&T Inc. and BellSouth Corp., Notice of Ex Parte Communication in WC Docket No. 06-74 (Dec. 28, 2006) (available at gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518716381) ("Offer of Conditions").

[10] FCC New Release, "FCC Approves Merger of AT&T Inc. and BellSouth Corporation; Significant Public Interest Benefits Likely to Result," WC Docket No. 06-74 (Dec. 29, 2006).

[11] AT&T Inc. Form 8-K (filed with the SEC on Dec. 29, 2006) (available at www.sec.gov/Archives/edgar/data/732717/000095012306015733/y28428e8vk.txt).

[12] See U.S. Department of Labor, Bureau of Labor Statistics, "Telecommunications" (available at

offshore outsourcing by U.S. telecommunications service providers – decreased network construction, industry consolidation by service providers, exit of some competitors, and implementation of more-automated and lower-maintenance technologies.[13] Yet, there had been some articles in 2004 on BellSouth's decisions to move 600-900 positions in information technology applications to India (with $275 million in savings over five years) and use foreign workers in help desk support for broadband customers.[14]

The Communications Workers of America (CWA) participated in the FCC's review of the AT&T/BellSouth merger. This labor union represented more than 175,000 employees at the merging companies.[15] CWA's comments pointed to AT&T's decision following the AT&T/SBC merger to close some U.S.-based call centers and contract with vendors based overseas to handle customer calls. The union noted its efforts to reach an agreement with the merging companies to protect employment security. In the absence of an agreement with the companies, CWA supported conditions to the FCC's approval such that the "merged entity does not sacrifice quality customer service by reducing employment and closing facilities to meet synergy targets."[16]

Second, the AT&T/BellSouth merger was approved by public utility commissions in nineteen states.[17] Conditions for approval of this transaction were adopted by some state

---

www.bls.gov/oco/cg/cgs020.htm) ("BLS Telecommunications") ("Employment in the telecommunications industry is expected to decline 7 percent over the 2004-14 period, compared with 14 percent growth in all industries combined."); Statement of Kathleen P. Utgoff, Commissioner, Bureau of Labor Statistics, before the Joint Economic Committee, U.S. Congress, "Employment Situation for September 2004" at 4 (Oct. 8, 2004) (available at 72.14.203.104/search?q=cache:rgdVwZhiTAIJ:jec.senate.gov/_files/utgofftestimony.pdf+senate+telecommunications+employment&hl=en&gl=us&ct=clnk&cd=3) (since March 2001, the telecommunications industry has shed 302,000 jobs); Remarks of FCC Chairman Michael K. Powell at the Goldman Sachs Communicopia XI Conference at 1 (Oct. 2, 2002) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-226929A1.pdf) (nearly 500,000 jobs lost in the telecommunications industry). In contrast, see note 1 to Chapter One, *supra* (FCC Chairman Martin: "In 2006,…job creation in the industry is high….").

[13] See BLS Telecommunications, *supra*; Written Statement of FCC Chairman Michael K. Powell before the Senate Committee on Commerce, Science and Transportation, "Financial Turmoil in the Telecommunications Marketplace: Maintaining the Operations of Essential Communications" at 6-10 (July 30, 2002) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-224797A1.pdf). Concerns about declining U.S. employment in the telecommunications industry had been voiced for several years at the FCC and in Congress. With Democrats capturing a majority of the Senate and House of Representatives in the November 2006 election, labor unions were poised to increase their influence on federal government decisions, including with regard to this issue.

[14] See Wreden, "Overseas outsourcing bites into telecom; political pressure keeps jobs here, but for how long?" America's Network (Feb. 15, 2004) (available at findarticles.com/p/articles/mi_m0DUJ/is_2004_Feb_15/ai_n6082741); E-Business Strategies, Inc., "BellSouth Corporation: The Telecommunications Industry Looks to Offshore IT" (2004) (available at www.ebstrategy.com/downloads/case_studies/Bellsouth.pdf).

[15] Comments of Communications Workers of America filed in WC Docket No. 06-74 at 1 (June 5, 2006) (available at svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518358746) ("CWA Comments").

[16] *Id.* at 4.

[17] Offer of Conditions, *supra*, at 1.

regulators, including to address labor concerns. For example, the Kentucky Public Service Commission's approval on July 25, 2006, included commitments by the merging parties to cap rates for basic local service for five years, maintain local charitable and economic development activities, adhere to labor agreements in place at the time of the merger, and notify the Kentucky commission prior to closing any facilities in the state.[18] It does not appear that any state commission required the merged company to increase employment in that state or addressed the repatriation of offshore outsourced jobs. While Louisiana would benefit from a particular provision in the companies' labor commitment to the FCC, the order adopted by the Louisiana Public Service Commission did not contain any condition related to jobs.[19]

3.2 Repatriation Condition in FCC's Order Approving the AT&T/BellSouth Transaction

The AT&T/BellSouth commitment which became a condition to the FCC's approval of the merger reads as follows:[20]

> AT&T/BellSouth is committed to providing high quality employment opportunities in the U.S. In order to further this commitment, AT&T/BellSouth will repatriate 3,000 jobs that are currently outsourced by BellSouth outside of the U.S. This repatriation will be completed by December 31, 2008. At least 200 of the repatriated jobs will be physically located within the New Orleans, Louisiana MSA.

Only Democratic Commissioner Copps—not his Democratic colleague or the Republican commissioners—pointed to this condition in his statement on the merger order.[21] The FCC order approving the transaction does not mention the repatriation condition in analyzing the potential public interest benefits or harms from the transaction. CWA praised the merger with the

---

[18] Kentucky Public Service Commission News Release, "PSC Approves BellSouth Merger with AT&T; Merger will have no immediate effect on rates" (July 25, 2006) (available at psc.ky.gov/agencies/psc/press/072006/0725_r01.pdf).

[19] AT&T, Inc. and BellSouth Corporation, La PSC Order No. U-29427 (July 12, 2006) (available at https://p8.lpsc.org/Workplace/getContent?objectStoreName=Orders&vsId=%7B1C0CB098-6248-4144-A7CA-E78E3A07765B%7D&objectType=document&id=%7B9624BD8E-9DA0-411A-BE89-A95BF697DFE1%7D). See also *Joint Application for Approval of Indirect Transfer of Control of Telecommunications Facilities Resulting from Agreement and Plan of Merger between AT&T Inc. and BellSouth Corporation*, FL PSC Order No. PSC-06-0531-PAA-TP (June 23, 2006) (available at www.psc.state.fl.us/library/filings/06/05491-06/06-0531.ord.doc) (finding the transfer of control to be in the public interest based on the companies' management, technical and financial capabilities; the companies' operations will remain intact while they project synergies of $2 billion annually; does not address employment effects).

[20] Offer of Conditions, *supra*, at 2. The conditions appear in Appendix F of the FCC's order approving the transaction. *AT&T Inc. and BellSouth Corporation Application for Transfer of Control*, FCC 06-189 (rel. Mar. 26, 2007) ("AT&T/BS Order").

[21] Copps Statement, *supra*, at 6. See Chapter One, note 6.

conditions, pointing to jobs created by the companies' commitment to expand broadband services as well as the "commitment to bringing thousands of support jobs back to the United States."[22]

The repatriation condition was adopted in the context of two findings in the FCC's order. First, the FCC found that the merger would promote national security.[23] Second, the FCC found that the merger would produce efficiencies related to vertical integration as well as economies of scope and scale (with much of the cost savings from head count reductions) that would benefit the public interest.[24]

3.2 Analysis of AT&T/BellSouth Conditions

The FCC's order approving the AT&T/BellSouth merger is notable on globalization issues from two perspectives. First, the commitment it adopts reversing some offshore outsourcing runs contrary to the policy of globalization. Second, while the FCC was well-aware of the conditions imposed in other FCC orders as a result of CFIUS reviews of some foreign acquisitions, the FCC did not adopt any of these national security conditions for this domestic merger.

3.2.1 Weak Linkage to National Security and Employment Security

The preceding sections noted the Congressional, FCC, and U.S. Trade Representative policies of deregulating carriers' decisions on services and networks, limiting regulatory burdens imposed on carriers' operations, and promoting the globalization of the telecommunications industry. The FCC previously allowed carriers to make unregulated, market-based decisions on where to conduct their operations, including through offshore outsourcing. Moreover, the U.S. government fought against restrictions by foreign governments on U.S.-produced equipment and services in foreign telecom sectors.

Although perhaps a reasonable political action to help organized labor, an important constituent in Democratic politics, the repatriation condition is contrary to these policies. In an attempt to cast of favorable light on this condition in the context of the FCC's established policies, Commissioner Copps linked the jobs repatriation condition to developing the next-

---

[22] See CWA, "AT&T-BellSouth Merger will Promote Critical Build-Out of High-Speed Networks" (Dec. 29, 2006) (available at /www.cwa-union.org/news/page.jsp?itemID=28161726).

[23] AT&T/BS Order, *supra*, at para. 208 ("We take considerations of national security and disaster recovery extremely seriously, and we find that the merger has the potential to generate significant benefits by enhancing national security, improving services to U.S. government customers, and enhancing the Applicants' disaster recovery capabilities. Specifically, we find that the merger will enable a unified, end-to-end, IP-based network that can provide the government with additional security and routing efficiency for vital and sensitive government communications. In addition, we find that the merger will enhance the Applicants' abilities to prepare for, and respond to, disasters.").

[24] *Id.* at para. 219.

generation of communications services in the United States[25] Yet, there is little to support this linkage.

Copps's assertion starts from the view that foreign workers contribute less to the development of U.S. telecommunications networks and services than do U.S. workers. In recent years, BellSouth sold most of its investments in foreign carriers to focus on its U.S. service providers and operations, including through the expansion of broadband services.[26] Facing increasing competition from cable television systems, wireless operators, voice over Internet Protocol services and other providers, BellSouth had strong incentives to innovate, improve quality and reduce prices (and costs) for its U.S. networks and services. When BellSouth decided to move offshore some support jobs that were tied to the U.S. networks and services, this market-based business decision was made through analysis of costs, availability of skilled workers, speed and quality of technology development, and quality of customer service – all for the benefit of BellSouth's U.S. networks and services.

In addition to taking advantage of an opportunity to help a U.S. labor union and U.S. workers, Copps may have believed that BellSouth diminished its efforts to develop next-generation services in the United States through its offshore outsourcing. If Copps believed that the market was failing in this area, the repatriation condition may do little to address concerns about service quality and network upgrades.

The condition does not specify the types of jobs that must be repatriated. As noted above, it appears from press articles that some of BellSouth's offshore support came in help-desk services while others worked in applications development.[27] The technology skills involved in help-desk jobs for broadband services (or billing inquiry positions, data entry, and various lower-skilled information technology jobs) are significantly different than the technology skills in software development positions (or network design, equipment development and other higher-skilled information technology jobs). Perhaps the merged company would repatriate jobs linked to developing next-generation services; on the other hand, the company did not agree to such

---

[25] See Copps Statement, *supra*, at 6. See also Institute of Electrical and Electronics Engineers (IEEE)-USA, "Position: Offshore Outsourcing" (Mar. 2004) (available at www.ieeeusa.org/policy/positions/offshoring.html) ("IEEE-USA is particularly concerned that offshoring of engineering, computer science and other high tech jobs could eventually weaken America's leadership in technology and innovation, a threat that has serious implications for our national security as well as our economic competitiveness.").

[26] See BellSouth Corp. 2005 Form 10-K/A at 3, 4, 6 (filed with the SEC on Mar. 1, 2006) (realigned asset portfolio toward domestic wireless and broadband, with sale of Latin American operations; business strategy includes "providing superior service and by offering flexible packages of voice, data and multimedia applications through improved distribution channels and systems", "deploying new broadband/[Internet Protocol] platforms that support both voice and data services as well as other new service applications" and "reduc[ing] our cost structure by managing the utilization of existing assets and redirecting spending to focus new investment on high-growth products and services"; BellSouth described increasing competition and price pressures).

[27] See note 14 to this chapter. BellSouth had taken measures to ensure the security of its Indian delivery center, such as regular employee background checks, physical security and a full disaster recovery plan.

linkage in the condition, and the 3,000 jobs that would be repatriated may have little to do with developing next-generation networks and services.

While complying with this condition, economics may drive the merged company to keep or move offshore many other positions that are key to developing the next-generation of U.S. communications services.[28] If the company cannot use offshore employees that it manages for technology development, it may attempt to achieve technology development at comparable costs by contracting with offshore equipment manufacturers. The merged company and U.S. carriers generally were acquiring technologies from a wide range of offshore suppliers.[29]

Although the FCC has found that improved network technologies and service quality can promote national security,[30] it is not clear that the repatriation condition will achieve this goal. By reversing free-market decisions to use offshore outsourcing, the condition will raise the merged company's costs. Also, the migration of jobs may disrupt some projects. While the public record does not include analysis by the FCC, the merged company or the CWA of the actions to comply with this condition and their impacts, these impacts may slow technology development and deployment, decrease the quality of support services for offerings, and lessen price competition.

According to CWA, the FCC must consider the employment impacts of mergers in determining whether transactions would serve the public interest.[31] The repatriation commitment does little to address employment security for the unionized workers of the merging companies. There is no overall commitment to employment in the United States; the merged company can proceed with its plan to cut 10,000 workers. Additionally, there is no restriction on new offshore or domestic outsourcing.

From the CWA's perspective, the repatriation condition may symbolize the ability of political pressures regarding U.S. employment to cause a giant U.S. telecom company to bend. On the other hand, it may also symbolize the limited power of U.S. labor unions and labor-oriented regulators in the increasingly global economy.

---

[28] See McDougall, "AT&T to Cut Hundreds of U.S. Tech Jobs, Sources Say" (Sep. 28, 2006) (available at www.ddj.com/dept/ai/193100354) ("AT&T's apparent decision to repatriate some jobs while outsourcing others reflects a growing dilemma faced by many U.S. companies.... AT&T has apparently decided to maintain customer-facing jobs in the United States while shipping out behind-the-scenes operations."; Programmers in India typically earn at least 60% less than their U.S. counterparts.).

[29] See Section 2.2.3.2 of this report.

[30] AT&T/BS Order, *supra*, at para. 209; SBC/AT&T, *supra*, at paras. 186-95; Verizon/MCI, *supra*, at paras. 197–207.

[31] CWA Comments, *supra*, at 3.

3.2.2 Failure to Consider National Security Measures Adopted in Foreign-Ownership Transactions.

The FCC adopted its order approving the AT&T/BellSouth merger two weeks after the Departments of Homeland Security and Justice filed with the FCC the Security Agreement as a proposed condition on the FCC's approval of the Verizon/América Móvil transaction. Over the past few years, the FCC had in several proceedings (each involving a foreign acquisition of a U.S. telecom carrier) adopted many of these conditions in security agreements developed pursuant to CFIUS reviews.[32] National security is a component of the FCC's public interest determination for domestic as well as cross-border transactions.[33] Yet, in the AT&T/BellSouth transaction creating the largest U.S. telecom carrier, the FCC did not adopt any of the CFIUS national security measures.

A foreign acquisition of a provider of U.S. infrastructure services may increase concerns about U.S. national security.[34] However, some of the CFIUS measures for foreign-acquired carriers could be viewed as industry best practices and helpful for U.S. law enforcement, whether implemented by a domestic or foreign-owned carrier.[35] These measures potentially include personnel screening; storing traffic and customer records in the United States; transmitting and controlling domestic traffic in the United States; appointing a qualified security officer with reporting obligations to the U.S. government; and annual third-party audits of security practices and vulnerabilities. For example, the FCC and national security agencies should be concerned about the ability of an untrustworthy employee to harm the U.S. communications infrastructure or disclose sensitive information, regardless of whether that employee gains access through a position at a domestic or foreign-owned carrier. An industry-wide approach to safeguards is especially warranted for the telecom industry in light of the interconnected, networked operations and services of multiple carriers.

In addition to possible national security benefits, a wider application of these conditions would have promoted the FCC's policies of fair competition and globalization.
Imposing these measures on domestic carriers would have leveled the competitive playing field with the foreign-acquired carriers that agreed to these measures in connection with recent acquisitions. The costs for U.S. national security measures would have fallen more equally across competitors. Also, a wider application of these measures would have sent the signal to foreign

---

[32] See DT, *supra*; *Applications of Guam Cellular and Paging, Inc. and DoCoMo Guam Holdings, Inc*., FCC 06-167 (2006); Lewis, *supra*.

[33] See AT&T/BS Order, *supra*, at para. 208; SBC/AT&T, *supra*, at paras. 186-89; Verizon/MCI, *supra*, at paras. 197-201 ("We take considerations of national security extremely seriously, and we find that the merger has the potential for greater benefits arising from more efficient routing and greater redundancy.").

[34] See note 32 and accompanying text, *supra*.

[35] The repatriation condition highlights the role of foreign workers and operations for U.S.-owned carriers. See note 14 to this chapter and Section 5.3 of this report.

governments that the United States does not unreasonably discriminate against foreign-owned carriers and foreign investors.

Nevertheless, there is no indication that the FCC considered imposing any of the CFIUS measures as conditions for the AT&T/BellSouth merger. None of the Departments of Homeland Security and Justice, other interested parties, legislators, foreign-owned carriers or the FCC itself pressed for these measures. Accordingly, the merging companies did not "offer" them.

Perhaps the FCC and the national security agencies were reluctant to pursue these measures for a domestic transaction in light of the Congressional and FCC policy of minimizing regulatory burdens.[36] It is also possible that these agencies decided that any expansion of these measures to domestic carriers should be done industry-wide through a statute or rulemaking, instead of as merger conditions. In any case, the absence of these conditions in the FCC's approval of the largest domestic telecom merger calls into question the balance struck in foreign acquisitions between national security concerns and policies favoring globalization and deregulation.

[36] See generally Lavey, "Responses by the Federal Communications Commission to WorldCom's Accounting Fraud," 58 *Fed. Com. L.J.* 613, 674–77 (2006).

Chapter Four

Foreign Responses and Context

Chapters Two and **Three** of this report described three transaction-specific conditions imposed by the U.S. government which sacrifice some aspects of telecom globalization and deregulation to promote national security and employment security. The next step in the analysis considers three points in the international context for these U.S. actions: (a) foreign responses to CFIUS-imposed conditions on telecom transactions; (b) foreign restrictions on acquisitions of infrastructure businesses by U.S. and other non-domestic companies; and (c) recent U.S. efforts to address foreign restrictions on telecom globalization. These points show that the there is significant international attention to CFIUS-imposed conditions on telecom transactions, with implications for foreign governmental actions with regard to telecom globalization, and that the United States continues to pursue commitments by foreign governments to open their telecom sector.

4.1 Foreign Responses to CFIUS-Imposed Conditions on Telecom Transactions

In 2005-06, U.S. concerns about foreign responses to CFIUS issues focused on the Congressional reactions to the proposed CNOOC/Unocal and Dubai Ports transactions as well as some of the bills introduced in Congress that would have sharply restricted foreign acquisitions of U.S. infrastructure businesses.[1] While not as significant as the concerns about those actions, foreign governments have noticed and objected to the CFIUS-imposed conditions on telecom transactions in the forms of security agreements.

In particular, the European Commission issued a report in February 2007 (after the CFIUS review of the Alcatel/Lucent transaction) which pointed specifically to these "far-reaching" agreements "impos[ing] strict corporate governance requirements on companies seeking [FCC] approval of the foreign takeover of a U.S. communications firm."[2] The report on U.S. barriers to trade and investment stated: "The EU recognizes that there are security issues to be resolved relating to trade and investment, particularly in the aftermath of 9/11, but has long expressed concern about excessive use which could be interpreted to be a disguised form of protectionism."[3]

---

[1] See, e.g., Letter from the Business Roundtable to Members of the United States Congress (Mar. 27, 2006) at 2 ("If the Congress were to adopt excessive changes, such as banning foreign investment in or across certain sectors, there is a significant risk that these types of changes would have the unintended consequence of discouraging legitimate foreign investment in the United States and encouraging other countries to discriminate against U.S. companies.")(available at www.businessroundtable.org/pdf/32706LettertoCongressCFIUSFINAL.pdf); Chapter Two, notes 7–10.

[2] European Commission, *United States Barriers to Trade and Investment: Report for 2006* at 14 (Feb. 2007) (available at trade.ec.europa.eu/doclib/docs/2007/february/tradoc_133290.pdf).

[3] *Id.*

Similarly, a 2005 report by the Commission of the European Communities (after the CFIUS reviews of the Deutsche Telekom/VoiceStream and Global Crossing/Singapore Technologies Telemedia/Hutchison Telecommunications transactions) pointed to the harms to investment flows from the types of conditions in the security agreements. In discussing "anomalous ownership restrictions on the US side which go beyond the minimum necessary for security reasons," but without singling out telecom transactions, the report stated: "EU Companies are also concerned that screening and notification procedures involving [CFIUS] include disproportionate oversight and corporate governance requirements, as well as screening of sensitive personnel."[4]

In addition to these statements by foreign governments objecting to excessive CFIUS-imposed conditions, these conditions have likely contributed to the increasing reviews of U.S. and other non-domestic investments by foreign governments, as discussed in the next section.

4.2 Foreign Restrictions on Acquisitions of Infrastructure Businesses

While the CFIUS-imposed conditions on telecom transactions conflict with globalization and deregulation policies, they are less restrictive than a prohibition on foreign acquisitions of U.S. businesses in this sector. Other countries have been protectionist in this sector, making the U.S. conditions appear less of an outlier or threat to globalization developments.

For example, French Decree No. 2005-1739 of December 2005 requires prior approval by the Minister of Economy for a non-EU entity to make an acquisition in one of the country's eleven "sensitive sectors" (or strategic domestic industries), which include telecommunications companies.[5] This policy has led some observers to the view that France would not have allowed Lucent to acquire Alcatel, even subject to national security safeguards in agreements.[6]

An article in early 2007 identified several major governments which scrutinize proposed significant foreign investments for potential national security impacts, including Canada, France, Germany, the United Kingdom, Russia, China, and India.[7] The authors observed: "The trend toward tighter review procedures suggests that the U.S. security concerns may be influencing other lawmakers and that there is a broader global trend to give security concerns greater weight in investment policy."[8] In one well-publicized matter in 2005, India's Foreign Investment

---

[4] Commission of the European Communities, *Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee: A stronger EU-US Partnership and a more open market for the 21st century* at 7 (May 2005) (available at trade.ec.europa.eu/doclib/docs/2005/may/tradoc_123438.pdf).

[5] Lichtenbaum & Irwin, "National Security Review of Foreign Investment: Recent Developments Around the World," 36 *Int. L. News* 13, 14 (2007) ("Lichtenbaum & Irwin").

[6] Hawkins, "Business Should Favor a Stronger CFIUS," at 2 (May 8, 2006) (available at defensenews.com/story.php?F=1760114&C=commentary).

[7] Lichtenbaum & Irwin, *supra*, at 13.

[8] *Id.*

Promotion Board and Department of Telecom stalled applications by the Chinese telecom equipment manufacturer Huawei Technologies Co. to set up a manufacturing unit as well as a research and development center in India and to bid on state telecom projects.[9] The reports refer to security concerns from India's intelligence agencies on Huawei's links to the Chinese intelligence and military establishments.

In addition to laws providing for reviews of foreign acquisitions in multiple sectors, some countries have laws or rules setting caps on foreign ownership of telecommunications companies.[10] In Canada, the Telecommunications Act requires that Canadians control and own at least 80 percent of the voting shares of a telecommunications common carrier.[11] A report by Canada's Standing Committee on Industry, Science and Technology in 2003 recommended that this restriction be eliminated, noting that the Investment in Canada Act subjected foreign acquisitions of Canadian businesses in all sectors to a "net benefit" review by the Minister of Industry.[12] Nevertheless, Canada has not changed its foreign ownership restrictions in the telecom sector.

4.3 Recent U.S. Efforts to Address Foreign Restrictions on Telecom Globalization

One more piece of the foreign context for the actions by CFIUS and the FCC is the U.S. government's continuing effort to obtain commitments by foreign governments to open their telecom sector. This effort is illustrated by the U.S. free trade agreement with the Republic of Korea announced on April 1, 2007.

In announcing the commencement of these negotiations with South Korea, the U.S. Trade Representative called them "the most commercially significant free trade negotiation we have embarked on in 15 years."[13] The announcement went on to state as background: "The United

---

[9] See, e.g., Basu, "Raising the red scare in India's telecom sector," Asia Times Online (Nov. 15, 2005) (available at www.atimes.com/atimes/South_Asia/GK16Df02.html); Ribeiro, "Plan from China's Huawei may be blocked in India," *Computerworld* (Aug. 17, 2005) (available at www.computerworld.com/managementtopics/outsourcing/story/0,10801,103990,00.html).

[10] The U.S. allows foreign ownership of common carriers in excess of 25 percent if the FCC finds that such ownership will serve the public interest, with a presumption in favor of the foreign ownership in cases of investment from countries which are signatories to the WTO's Basic Telecommunications Agreement. See Chapter One, note 7; FCC International Bureau, "Report on International Telecommunications Markets 2000 Update" at 3-4, DA 01-117 (May 4, 2001).

[11] International Telecommunication Union, "ICT Regulation Toolkit Practice Note: Foreign Ownership in Canada [3.4.2]" (available at www.ictregulationtoolkit.org/en/PracticeNote.1882.html).

[12] *Id.* The report found that restrictions on foreign investment in the sector impeded capital investment by new entrants, growth and productivity.

[13] United States Trade Representative, "United States, South Korea Announce Intention to Negotiate Free Trade Agreement" (Feb. 2, 2006) (available at www.ustr.gov/Document_Library/Press_Releases/2006/February/United_States,_South_Korea_Announce_Intention_to_Negotiate_Free_Trade_Agreement.html?ht=).

States is aggressively working to open markets globally, regionally and bilaterally and to expand American opportunities in overseas markets"[14]

The Business Roundtable urged the U.S. negotiators to identify and remove non-traditional barriers to the Korean market.[15] This report cited the existence of technical barriers in many sectors of Korea through laws or regulations that appear neutral on their face but have the effect of excluding U.S. products or making them less competitive. Specifically in the telecommunications sector, this U.S. group claimed that Korea began setting standards for next-generation equipment and technology in a manner favoring Korean technology.[16]

As announced on April 1, 2007, the free trade agreement includes three commitments by Korea in the telecom sector: (a) permit U.S. companies within two years to own up to 100 percent of a telecommunications operator in Korea; (b) provide U.S. operators cost-based access to the services and facilities of dominant Korean telephone companies, including submarine cable stations, to facilitate the U.S. companies' construction and operation of competing networks to serve customers in Korea; and (c) "groundbreaking safeguards" on restrictions that regulators can impose on operators' technology choice, particularly in wireless technologies.[17]

As part of the support for this agreement, AT&T commended the U.S. Trade Representative's "ongoing commitment to promote competition and encourage investment in global telecommunications markets," and called for rapid approval of the agreement by the lawmakers in the United States and Korea to "ensure that consumers everywhere reap the benefits of a fully competitive global telecommunications environment."[18] Similarly, the Telecommunications Industry Association, representing telecom equipment manufacturers in the United States, observed that the agreement will "let the people of both nations continue to use the latest in [information and communication technology] ICT products."[19]

In summary, the U.S. Trade Representative continues to pursue open global telecommunications markets. The CFIUS and FCC actions described in **Chapters Two** and

---

[14] *Id.*

[15] Business Roundtable, "Real Liberalization in the U.S.-Korea FTA: Moving Beyond the Traditional FTA" at 6 (June 2006) (available at 64.203.97.43/pdf/20060607000korea_paper.pdf).

[16] *Id.* at 7.

[17] United States Trade Representative, "Free Trade with Korea: Summary of KORUS FTA" at 4 (April 1, 2007) (available at www.ustr.gov/assets/Document_Library/Fact_Sheets/2007/asset_upload_file939_11034.pdf); "Proposed United States-Korea FTA Texts" (May 24, 2007) (available at www.ustr.gov/Trade_Agreements/Bilateral/Republic_of_Korea_FTA/Draft_Text/Section_Index.html).

[18] United States Trade Representative, "Strong Support for the U.S.-Korea (KORUS) Free Trade Agreement" at 5 (May 24, 2007) (available at www.ustr.gov/assets/Document_Library/Fact_Sheets/2007/asset_upload_file608_11053.pdf).

[19] *Id.* at 4.

Three of this report do not appear to have impeded the progress in this area reflected in the U.S.-Korea free trade agreement. On the other hand, other governments have objected to the CFIUS-imposed restrictions in the telecom sector, and have increased their reviews of acquisitions by U.S. and other non-domestic companies in the telecom and other sectors.

Chapter Five

Addressing National Security Vulnerabilities Through Industry-Wide Measures

The restrictions described in **Chapters Two** and **Three** were adopted on a transaction-specific basis, applying to only a few companies in a multi-carrier, multi-supplier, networked industry. The resulting spotty efforts to address national security vulnerabilities or offshore outsourcing not only imposed heavier burdens on the merging companies, but also left large gaps in pursuit of those policy objectives. The analysis referred to the possible alternative of the U.S. government taking an industry-wide approach to these policy objectives. In fact, there have been industry-wide national security efforts which were intensified post-9/11 through laws, regulations and government-led plans in the many infrastructure industries, including the telecommunications sector.[1] While the types of measures agreed to in the TELPRI Security Agreement have been applied to some industries, those types of protections have not been applied across telecommunications services or equipment companies. This section describes national security protections in four other industries, the increased security measures imposed on foreign-owned contractors for U.S. classified projects, and the limited scope of the industry-wide security practices for the telecommunications industry.

5.1 National Security Protections in Some Industries

Congress and regulatory agencies have adopted legislation and rules applying to several industries security measures such as personnel screening, company-developed and government-reviewed security plans, physical and information-systems access controls, and company security officers. These requirements do not single out foreign-owned firms. This section briefly reviews some of the industry-wide measures in several infrastructure sectors -- marine ports, airports, nuclear power plants, and financial institutions.

5.1.1 Marine Ports

U.S. marine ports have a mix of foreign and domestic ownership, reflecting the globalization of shipping lines, supply lines and distribution networks.[2] Congress has taken an

---

[1] See Department of Homeland Security, "National Infrastructure Protection Plan" (2006) (available at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf); DHS Press Release, "Remarks of Secretary Michael Chertoff at a U.S. Chamber Event on the Completion of the 17 Sector Specific Plans, as Part of the National Infrastructure Protection Plan" (May 21, 2007) (available at www.dhs.gov/xnews/speeches/sp_1179843074582.shtm); Homeland Security Presidential Directive/Hspd-7 (Dec. 17, 2003) (available at www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

[2] See CRS Report for Congress, "Terminal Operators and Their Role in U.S. Port and Maritime Security" at 3-4 (Apr. 20, 2006) (available at http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-9273:1) ("CRS Report") (according to a survey by the U.S. Maritime Administration, at the 17 largest U.S. container ports, 66% of the terminals are operated by a foreign-owned company, 26% are run by purely domestic companies, and 7% are run by a domestic/foreign joint venture; "Foreign involvement in U.S. port terminal operations is an extension of an industry

industry-wide approach to tightening security at marine ports facilities, with the same requirements applicable regardless of the nationality of ownership.

Congress adopted laws requiring additional security measures for marine ports in the Maritime Transportation Security Act of 2002[3] and the Security and Accountability for Every Port Act of 2006.[4] One major initiative is a personnel security program administered by the Transportation Security Administration (TSA). Under a rule adopted by the Department of Homeland Security, TSA and the U.S. Coast Guard in January 2007, an estimated 750,000 individuals will require Transportation Worker Identification Credentials.[5] The program covers merchant mariners and workers with unescorted access to secure areas of vessels and port facilities, and requires individuals to undergo a security threat assessment and receive a biometric credential. Enrollment and issuance of credentials is planned to occur over an 18 month period.

The 2002 law also requires marine ports to develop security plans that are subject to initial review, approval and periodic inspection/review by the Department of Homeland Security, implemented through the U.S. Coast Guard.[6] The plans include a security officer; vulnerability assessment; physical, cargo and personnel security measures, including security training for all personnel as well as drill and exercise requirements; access controls to secure areas; record keeping and monitoring requirements; and procedural security policies.

Some analysts have questioned whether there is a connection between U.S. national security and foreign ownership of marine ports. In one insightful passage, the authors of a Congressional Research Service report question the factual basis for singling out foreign-owned businesses for more extensive security measures:[7]

> It is important to pinpoint exactly what advantage a terrorist group would have if it had some kind of connection with a terminal operator. Foreign terminal operators would gain intimate knowledge of the day-to-day

---

driven by globalization. The largest container shipping lines have extended their services around the globe because their biggest customers, such as big box retailers and auto, electronics, and clothing manufacturers, have extended their supply lines and distribution networks around the globe."); Gilroy & Summers, "Detailing Foreign Management of U.S. Infrastructure; Numerous U.S. ports, airports, roads, water facilities already run by foreign businesses" (Mar. 15, 2006) (available at www.reason.org/phprint.php4) ("Gilroy & Summers").

[3] P.L. 107-295, 46 U.S.C. §§ 70101 et seq.

[4] P.L. 109-347.

[5] Department of Homeland Security, "Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License" (rel. Jan. 1, 2007) (available at www.tsa.gov/assets/pdf/1652-AA41_twic_fr.pdf); 46 U.S.C. § 70105; Transportation Security Administration, "Transportation Worker Identification Credential (TWIC) Program" (available at www.tsa.gov/what_we_do/layers/twic/index.shtm).

[6] 46 U.S.C. § 70103(c); 33 C.F.R. Part 105.

[7] CRS Report at 13.

> security procedures at the U.S. terminals they operate and theoretically could pass this knowledge on to a terrorist group. However, U.S.-based terminal operators would have the same knowledge and a terrorist group could infiltrate them also. Because foreign terminal operators hire mostly Americans to work in their terminals, they may pose no more security risk than a U.S.-based company. One could view foreign companies like DP [Dubai Ports] World as mostly the financiers behind the terminal operation with little or no involvement in the day-to-day running of the terminals.... [T]he issue of foreign terminal operators involves guaranteeing security while remaining attractive to sources of capital.

5.1.2 Airports

Like marine ports, security measures at U.S. airports combine personnel screening by the TSA and security plans developed by facility operators which are subject to government review and audit. Again, the requirements apply across airports operated by domestic and foreign companies. Several U.S. airports are operated or managed by foreign-owned companies.[8]

Pursuant to the Aviation and Transportation Security Act of 2001,[9] TSA works with airlines and airports in screening all airline and airport employees and contractors who require unescorted access to secure areas. Security Identification Display Area badges (695,564 active as of January 31, 2006) are required to access areas beyond alarmed doors that are used for airport operations, allowing access to the flight line, ramp or aircraft; in addition, sterile area badges (85,013 active as of January 31, 2006) are required to access areas beyond the passenger screening checkpoint but inside the terminal area.[10] Prior to employment, airlines and airports send fingerprints and other biographical information to the American Association of Airport Executives Transportation Security Clearinghouse, which transmits the information to TSA. TSA conducts a name-based security threat assessment against approximately ten databases, and updates these searches continuously for all cleared personnel. Also, TSA transmits to the Federal Bureau of Investigation (FBI) the necessary biographical information and fingerprint data to conduct criminal history records checks. As of April 2006, TSA was vetting approximately 1,100 applicants each week.

Airport operators are required to develop, submit for TSA approval and implement airport security programs.[11] The airport security programs must include an airport security coordinator;

---

[8] Gilroy & Summers, *supra*.

[9] P.L. 107-71, 49 U.S.C. §§ 114 *et seq.*

[10] Testimony of R. Jamison (Deputy Administrator, TSA) Before the U.S. House Committee on Government Reform, Subcommittee of Federal Workforce and Agency Organization (Apr. 4, 2006) (available at www.tsa.gov/press/speeches/asset_summary_multi_image_with_table_0393.shtm).

[11] 49 C.F.R. § 1542.

personnel screening and identification; inspections/audits by TSA; descriptions of the secured areas; access control measures; training programs; and record keeping systems.

5.1.3 Nuclear Power Plants

Section 103d of the Atomic Energy Act of 1954, as amended, provides that no license for a nuclear power plant may be issued to an alien, or to a corporation owned, controlled, or dominated by an alien, foreign corporation, or foreign government.[12] The Nuclear Regulatory Commission (NRC) issued guidelines in 1999 providing for a range of foreign investments in utilities as long as the companies remain under the control and domination of U.S. citizens,[13] and has approved some foreign minority interests.[14] With the limited foreign ownership interest in this sector, the point of the following description is not the application of safeguards to foreign-owned as well as U.S.-owned operators, but rather the extensive government efforts to safeguard this infrastructure sector of U.S.-controlled operators.

In response to the September 11, 2001, attacks, the NRC ordered all operating nuclear power plants to submit revised physical security plans, safeguards contingency plans, and guard training and qualification plans.[15] The NRC developed and imposed a revised Design Basis Threat, and required licensees to address in their plans how they would protect against that threat.[16] In general, the changes resulted in more restrictive site access controls for personnel, including expanded, expedited and more thorough employee background checks; increased security patrols and posts; augmented security forces and capabilities; additional physical barriers; enhanced coordination with law enforcement and military authorities; and augmented security and emergency response training, equipment and communication.[17]

---

[12] 42 U.S.C. §2133(d).

[13] NRC, "Final Standard Review Plan on Foreign Ownership, Control or Domination," 64 Fed. Reg. 52355 (1999); 10 C.F.R. §50.38.

[14] See, e.g., *TMI Unit 1 Order*, Dkt. No. 50-4289 (Apr. 12, 1999); *Northeast Nuclear Energy Company; Order Approving Application Regarding Merger of New England Electric System and The National Grid Group PLC*, Dkt. No. 50-423 (Dec. 10, 1999); NRC Policy Issue Information, "Assessment of the Possible Effects of Nuclear Industry Consolidation on NRC Oversight" at 58-60, SECY-02-0143 (July 26, 2002).

[15] NRC Order EA 03-086, "Revised Design Basis Threat Order," 68 Fed. Reg. 24,517 (2003).

[16] See Statement of L. Reyes (Exec. Dir. for Operations, NRC) Before the U.S. House Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Homeland Security: Monitoring Nuclear Power Plant Security" 15-16 (Sept. 14, 2004) (available at www.nrc.gov/reading-rm/doc-collections/congress-docs/congress-testimony/2004/9-14-04-final.pdf).

[17] *Id.*; see also U.S. Government Accountability Office, "Nuclear Power Plants: Efforts Made to Upgrade Security, but the Nuclear Regulatory Commission's Design Basis Threat Process Should be Improved" (Mar. 2006) (available at www.gao.gov/new.items/d06388.pdf).

Congress also enacted industry-wide measures designed to improve the security of nuclear power plants and materials. Sections of the Energy Policy Act of 2005[18] expanded the scope of personnel subject to fingerprinting and criminal background checks by the FBI and the NRC; allowed the NRC to authorize licensees to use enhanced weapons; and established a system of manifests related to transfer or receipt of nuclear materials, with security background checks.

5.1.4 Financial Institutions

Banks and other financial institutions operating in the United States include a wide range of foreign-owned companies as well as diverse U.S. owners.[19] Concerned about the security of customer information obtained by all companies in this industry regardless of the nationality of ownership, Congress passed in the Gramm-Leach-Bliley Act of 1999 a provision requiring the Federal Trade Commission (FTC) to establish standards relating to administrative, technical and physical information safeguards for financial institutions.[20] This provision has been implemented through a "softer" industry-wide requirement of security measures compared to the mandates described above for marine ports, airports and nuclear power plants—fewer specific government-ordered security requirements, and a smaller role for government agencies in reviewing security plans and performing security checks.

Clearly, there is a huge difference in national security importance between safeguarding an individual consumer's checking account information versus protecting the major operations of a marine port, airport, nuclear power plant or financial institution.[21] The point here is to contrast both the approach and measures of the CFIUS transaction-specific conditions pertaining to telecommunications call records against the industry-wide statute and rule for protecting financial institutions' customer information.

The Safeguards Rule adopted by the FTC requires financial institutions to develop written information security plans that describe their programs to protect customer information, but allows flexibility in light of the entities' varying size, complexity, nature and scope of their activities, sensitivity of their customer information and other conditions.[22] The five components of

---

[18] P.L. 109-58, §§ 652-56. See NRC, Office of Nuclear Reactor Regulation, "Environmental Assessment Supporting Proposed Rule, Power Reactor Security Requirements" ii (May 2006) (available at www.nrc.gov/reading-rm/doc-collections/commission/secys/2006/secy2006-0126/enclosure4.pdf).

[19] See generally Federal Reserve Bank of San Francisco, "Patterns in the Foreign Ownership of U.S. Banking Assets," FRBSF Economic Letter 2000-35 (Nov. 24, 2000) (available at www.frbsf.org.econrsrch/wklyltr/2000/el2000-35.html).

[20] 15 U.S.C. §§ 6801-09.

[21] National security safeguards for financial institutions extend beyond protecting the privacy and security of customers' information to protecting the financial institutions' operations. See Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, "2006 Annual Report" (available at www.fsscc.org/reports/2006/annual_report_2006.pdf).

[22] FTC, "Standards for Safeguarding Customer Information," 67 F.R. 36484 (May 23, 2002); 16 C.F.R. Part 314;

each plan required by the FTC's rule are: (a) designate one or more employees to coordinate the safeguards; (b) identify and assess the risks to customer information, and evaluate the effectiveness of current measures; (c) design, implement, monitor and test a safeguards program; (d) hire appropriate service providers and contract with them to implement safeguards; and (e) periodically evaluate and adjust the program. Among other recommendations, the FTC suggests that companies consider (but does not require them to implement) checking backgrounds before hiring employees who will have access to customer information, training employees, and limiting access to sensitive customer information through physical locks and passwords.

Among the contrasts between the Safeguards Rule and the call-records provisions of the TELPRI Security Agreement are that the Safeguards Rule applies to all financial institutions subject to the FTC's jurisdiction, regardless of nationality of ownership; does not restrict the storage of customer records to domestic locations; recommends, but does not require, screening personnel with access to such records, and does not provide a role for a government agency in such screening; and does not require retention of records for five years.

5.2 Restrictions on Foreign-Owned Contractors for U.S. Classified Projects

One area of U.S. regulations which imposes additional security restrictions on foreign-owned firms involves contractors and subcontractors performing classified work for the U.S. government.23 Because of the representation on CFIUS of the Department of Defense and other agencies experienced in protecting classified work, this National Industrial Security Program (NISP) model has influenced both the transaction-specific approach and conditions adopted by CFIUS for certain foreign acquisitions, even when no classified work is performed by the target U.S. businesses. Yet, there are important distinctions between the treatment of foreign-owned firms under the NISP versus CFIUS-imposed provisions like those in the TELPRI Security Agreement.

The NISP requires all firms having access to classified information to implement a range of security measures. Regardless of the nationality of the owners, these measures include appointing a U.S. citizen employee who has a security clearance to supervise and direct security measures related to the classified information; adopting written security procedures if requested by the government agency; working with the government agency to screen personnel; providing security training to employees; cooperating with government representatives on inspections and security reviews; establishing physical protections and information system controls to safeguard classified

---

FTC Facts for Business, "Financial Institutions and Customer Information: Complying with the Safeguards Rule" (Apr. 2006) (available at www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.shtm); Testimony of O. Swindle (FTC Commissioner) Before the U.S. House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, "Protecting Our Nation's Cyberspace" (Apr. 21, 2004) (available at www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf).

[23] National Industrial Security Program, "Operating Manual," DoD 5220.22-M (Feb. 2006) (available at www.dtic.mil/whs/directives/corres/html/522022m.htm).

information, including publishing an information systems security policy and appointing an information systems security manager; implementing systems to minimize classified visits, including determining whether a visit is necessary, identifying visitors and limiting the disclosure of classified information based on need-to-know; and protecting against unauthorized exports of classified information or articles, or unauthorized disclosures to foreign interests.[24]

The additional measures applied to foreign-owned contractors for classified projects do not substantially increase the burdens of these day-to-day operational safeguards. Rather, the NISP largely addresses foreign ownership, control or influence in terms of the composition of the contractor's board of directors, the voting rights of the foreign shareholder and security responsibilities of certain directors.[25] A Special Security Agreement preserves the foreign owner's right to be represented on the board with a direct voice in business management while denying unauthorized access to classified information; it requires certain board members to be cleared U.S. citizens who are involved in security matters, and provides for the establishment of a Government Security Committee to oversee classified and export control matters. If the agency determines that national security requires greater insulation of the foreign owner from the business, then a Proxy Agreement requires the foreign owner to convey its voting rights to the proxy holders, who are cleared U.S. citizens having substantial freedom to manage the business independently of the foreign owner. As for supplemental operational safeguards, these agreements require the contractor to adopt a technology control plan approved by the agency for compliance with export restrictions, and to appoint a technology control officer. Most of the operational protections of classified information and restraints on the contractor's day-to-day functioning apply regardless of the nationality of ownership.

In contrast, the TELPRI Security Agreement imposes on the foreign-owned telecommunications carrier a wide range of operational safeguards as well as restrictions on the board of directors that do not apply to U.S.-owned carriers. The Security Agreement follows the NISP model by requiring the foreign shareholder to appoint certain directors who are U.S. citizens with security clearances and who have certain security responsibilities. On the other hand, the Security Agreement imposes burdensome conditions on the carrier's day-to-day functioning which are not applied to U.S.-owned firms. U.S.-owned carriers are not required to use only transmission, switching and hosting equipment located in the United States, or to store all records in the United States; they are not required to screen personnel; and they are not required to retain a neutral third party to perform annual security audits.

---

[24] *Id.* at 1-2-1, 2-2-1, 5-1-1, 5-2-1, 6-1-1, 8-1-1 and 10-2-1.

[25] *Id.* at 2-3-1 to 2-3-5.

5.3 Communications Sector Security Plan

On May 21, 2007, the U.S. Department of Homeland Security announced the completion of seventeen sector-specific plans for protecting the nation's critical infrastructure, including a plan for the communications sector.[26]

The communications sector plan (CS Plan) was developed through broad collaboration by government agencies and industry representatives.[27] The security strategy is aimed at ensuring that "the Nation's communications networks and systems are secure, resilient, and rapidly restored after an incident."[28] In the vision statement, protective programs (government and industry collaboration) focus on response and recovery strategies, while the industry (owners and operators) is responsible for employing prevention and protection strategies, and customers are responsible for protecting their assets and access points as well as providing for diverse and assured communications to support their essential functions.[29]

The CS Plan includes analyses of the sector's assets, risks, infrastructure prioritization, coordination programs and other important national security issues. For purposes of this report, review of the CS Plan will focus on the extent to which this plan applies industry-wide the types of measures that are applied through the CFIUS process only to a few foreign-owned companies. If so, then this government/industry effort would recognize that these CFIUS-imposed measures address important security vulnerabilities that should be implemented by all companies in this sector, and may decrease claims by foreign governments that requirements like the TELPRI Security Agreement erect a barrier to trade and investment by imposing heavier burdens on foreign companies.

Regarding industry protective measures and initiatives, the CS Plan refers to the efforts of an FCC advisory group to develop best practices -- recommendations for voluntary actions by infrastructure owners and operators which provide companies with guidance aimed at improving the overall reliability, interoperability and security of networks.[30] The protective measures fall into three categories: physical security, cyber/logical security, and human security. The CS Plan notes that companies vary in the protections they implemented depending on various factors.

---

[26] DHS News Release, "DHS Completes Key Framework for Critical Infrastructure Protection" (May 21, 2007) (available at www.dhs.gov/xnews/releases/pr_1179773665704.shtm); DHS News Release, "Fact Sheet: National Infrastructure Protection Program Sector-Specific Plans; U.S. Critical Infrastructure Sectors Formalize Risk-Reduction Roadmaps" (May 21, 2007) (available at www.dhs.gov/xnews/gc_1179776352521.shtm).

[27] Communications Sector Plan, *supra*, ii - iv (signatories include Departments of Homeland Security, Justice, Defense and Commerce; FCC; General Services Administration; National Telecommunications and Information Administration; New Jersey Board of Public Utilities; and the Communications Sector Coordinating Council (carriers, manufacturers and other service providers)).

[28] *Id.* at 2.

[29] *Id.* at 19, 25-26.

[30] *Id.* at 48, 109 (FCC's Network Reliability and Interoperability Council).

The best practices referenced by the CS Plan cover a wide range of topics for various categories of companies. For a wireline network operator like TELPRI, the website shows 639 best practices as of May 31, 2007.[31] Generally, the best practices -- even as voluntary recommendations for consideration by companies -- do not go as far as the Security Agreement.

For example, a best practice developed by the FCC advisory group regarding personnel screening states: "Network Operators, Service Providers, Equipment Suppliers and Property Managers should consider establishing and implementing background investigation policies that include criminal background checks of employees. The policy should detail elements of the background investigation as well as disqualification criteria."[32] In contrast, the Security Agreement requires more extensive screening (including background and financial investigations as well as criminal records checks by a third party, with regular monitoring of employees for possible disqualifications) with a greater involvement of government agencies (including that the company provides them the results of the third-party screening, and further background checks by government agencies).[33] These provisions of the Security Agreement appear to be closer to the Transportation Worker Identification Credential program or the screening for airport employees described above[34] than they are to the applicable voluntary best practices recommendation for the communications industry.

Certain best practices provide recommendations on network routing.[35] However, none of these recommendations even suggests that all companies consider the security benefits of the

---

[31] See Network Reliability and Interoperability Council, "Best Practices" (available at www.fcc.gov/nors/outage/bestpractice/ProcessBestPractice.cfm?RequestTimeout=500) ("NRIC").

[32] *Id.* at 7-7-5033. See also *Id.* at 7-7-8099 ("Network Operators, Service Providers and Equipment Suppliers should perform background checks that are consistent with the sensitivity of the position's responsibilities and that align with [human resources] policy. These checks could include those that verify employment history, education, experience, certification, and criminal history. ").

[33] TELPRI Security Agreement, *supra*, at 14-16 (screening through a reputable third party of existing personnel and new candidates in a list of positions developed through consultation with certain government agencies, including employees who have access to the communications infrastructure, call records, subscriber records or information on law enforcement activities; screening must include a background and financial investigation as well as a criminal records check; at the request of the government agencies, results of the screening will be provided to those agencies, and the employees and candidates must consent to such disclosure; cooperate with any federal government agency desiring to perform further background checks; candidates who are rejected by the government pursuant to such further background checks will not be hired or will be promptly removed from such position; monitor the screened personnel (update the screening), and promptly remove personnel who no longer meet the requirements; and maintain records on the status of screened personnel and provide them to government agencies on request).

[34] See Sections 5.1.1 and 5.1.2 of this report.

[35] NRIC, *supra*, at 7-7-0520 ("Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting."), 7-7-0566 ("Network Operators and Service Providers should consider placing and maintaining 911 circuits over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof)."), 7-7-0617 ("Network Operators and Service Providers should ensure that routing controls are implemented and managed to

location restrictions under the Security Agreement, that all equipment used to transmit, switch, control, manage or supervise domestic communications be located in the United States[36] On the contrary, one of the best practices addresses foreign sites and merely recommends a physical security program for such assets and personnel.[37]

A third example of these disparities is in the retention of records. The Security Agreement requires that this foreign-owned company store exclusively in the United States all domestic communications, call records, billing records and other subscriber information, and retain such information for at least five years.[38] Again, the best practices make several recommendations for all companies with regard to records, but do not suggest consideration of the security benefits of domestic-only storage and retention for at least five years.[39]

Finally, unlike the Security Agreement's restriction on outsourcing[40] and Commissioner Copps' discussion of the harms of offshore outsourcing, the best practices only address outsourcing in recommending consideration of a quality assessment, functional testing and security testing by an independent entity.[41]

In summary, the CS Plan and the compilation of voluntary best practices referenced therein reflect a major effort to promote national security by addressing all companies in the U.S. communications sector, U.S.-owned as well as foreign-owned. However, there are sharp disparities between the measures recommended therein for voluntary adoption by the entire

---

prevent adverse routing conditions."), 7-7-0731 ("Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis."), 7-7-1065 ("Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity."), 7-7-5105 ("Network Operators and Equipment Suppliers should consider the security implications of equipment movement both domestically and internationally, including movement across borders and through ports of entry."), and 7-7-5107 ("Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.").

[36] TELPRI Security Agreement, *supra*, at 7.

[37] NRIC, *supra*, at 7-7-5220 ("Network Operators, Service Providers and Equipment Suppliers who utilize foreign sites should establish and implement a comprehensive physical security program for protecting corporate assets, including personnel, at those sites.").

[38] TELPRI Security Agreement, *supra*, at 8-9.

[39] NRIC, *supra*, at 7-6-1022 ("Network Operators, Service Providers and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts."), and 7-7-3217 ("Network Operators and Service Providers should provide and maintain current 24/7/365 contact information accessible to Public Safety Answering Points (PSAPs) so that PSAPs may obtain additional subscriber information as appropriate.").

[40] TELPRI Security Agreement, *supra*, at 19.

[41] NRIC, *supra*, at 7-7-5084 ("Network Operators, Service Providers and Equipment Suppliers should consider ensuring that outsourcing of hardware and software includes a quality assessment, functional testing and security testing by an independent entity.").

industry versus the requirements imposed through the CFIUS process on a foreign-acquired company. The laws and regulations applicable to security measures for the marine ports, airports, and nuclear power plants industries are more stringent than the safeguards for the U.S.-owned telecommunications operators. These other sectors illustrate that Congress and federal agencies know how to make safeguards like those in the Security Agreement applicable industry-wide, but have failed to do so in the telecommunications sector.

Chapter Six

Conclusion

There is a complex, evolving fit for the telecommunications industry between (a) national security or employment security concerns and (b) policies favoring globalization and deregulation. Much is at stake in achieving this fit.

In Congressional testimony on February 7, 2007, the Treasury Department expressed concerns about deterring foreign investment and thereby weakening national security:

> The administration views investment, including investment from overseas, as vital to continued economic growth, job creation, and building an ever-stronger America.... As [Treasury] Secretary [Henry] Paulson has stated: "The U.S. experience illustrates the benefits of openness and competition. Our economy is by far the world's strongest because it is built on openness -- openness to people of all nationalities, openness to new ideas, openness to investment, and openness to competition."...
>
> [W]e have experienced recent controversies relating to particular foreign investments in the United States. These controversies, coupled with some troubling signs that other countries are pursuing barriers to foreign investment, and increasingly negative media coverage of the U.S. investment climate, underscore the need to improve and reform the CFIUS process....
>
> The administration regards our nation's security as its top priority....
>
> [L]et me emphasize that the Bush administration is firmly committed to keeping the U.S. economy open to international investment while at the same time protecting our national security. Openness at home encourages other nations to lower their barriers which can help advance prosperity and economic freedom in the rest of the world. In short, a domestic climate conducive to foreign investment strengthens national security.[42]

Despite the flurry of legislative proposals to reform the CFIUS process, there has been no legislative or regulatory effort to level the national security protections from CFIUS reviews across all foreign-owned and U.S.-owned telecommunications companies.43 Such

---

[42] Testimony of Treasury Assistant Secretary Clay Lowery before the House Financial Services Committee on the Committee on Foreign Investment in the United States at 2, 5 (Feb. 7, 2007) (available at www.house.gov/apps/list/hearing/financialsvcs_dem/htlowery020707.pdf). See also Paulson, *supra*, at 1-2 ("[T]he fear of foreign investment may be resurfacing….[W]e must assess the cost versus the benefits of our regulatory structure and certain aspects of our legal system that may discourage foreign investment.").

[43] Many of the Security Agreement-type CFIUS conditions date back to 2000 in the agreement covering NTT's acquisition of Verio. Lewis, *supra*, 57 *Fed. Com. L.J.* at 470-71. Yet, in over six years, Congress and the FCC have not applied such national security measures to all domestic and foreign-owned companies. While CFIUS has imposed these and additional conditions on several foreign acquirers of telecom and Internet service providers since the NTT/Verio

leveling of national security burdens regardless of nationality of ownership (at least for friendly foreign countries) would signal that the U.S. economy is open to international investment while strengthening national security.

Regarding the CFIUS recommendation on the Alcatel/Lucent transaction, President Bush proclaimed that CFIUS had properly balanced these interests: "The President's decision demonstrates the commitment of the United States to protect its national security interests and maintain its openness to investment, including investment from overseas, which is vital to continued economic growth, job creation, and an ever-stronger nation."[44] The signal sent by the National Security Agreement and Special Security Agreement is clearly more positive for foreign investment than if the President had blocked this transaction.

Perhaps the national security and employment security measures in the Verizon/América Móvil, Alcatel/Lucent and AT&T/BellSouth transactions achieve the optimal balance of these policies. On the other hand, there may be adverse effects in the actions of other governments against U.S. companies as well as decreased domestic competition and network upgrades. Recently-developed conditions on a few telecom companies are contrary to, or at least point in a different direction than, policies favoring globalization and deregulation that were developed and fought for over several decades by Congress, the FCC and other federal agencies. There should be further public scrutiny by Congress, the FCC and other agencies of the costs, benefits and implications of these measures. If these measures are found to promote national security in this multi-carrier, multi-supplier, networked industry, the public debate should address whether they should be applied to domestic companies as well.

Technology platforms for some telecom services have converged.[45] Similarly, some regulatory treatments for technically distinct but competing services have converged.[46] Yet, there is a growing divergence in national security conditions for U.S.-owned versus foreign-owned providers. At some point, this disparity may become harmful to the U.S. government's efforts to

---

agreement, these conditions do not apply to many foreign-owned service providers and do not apply to domestic-owned service providers. See also D. Heyman, "Ensuring National Security While Promoting Foreign Investment in an Age of Global Terrorism," Statement before the House Financial Services Committee at 4, 5 (Feb. 7, 2007) (available at www.house.gov/apps/list/hearing/financialsvcs_dem/htheyman020607.pdf) (lessons from the CFIUS review of the Dubai Ports transaction in 2006: "Foreign ownership does not and should not be assumed to automatically confer additional vulnerability on a business.... The threshold test for [CFIUS] national security reviews should be based on two assurances: one, that security of business transactions meet U.S. standards; and two, that U.S. government has the ability and authority to audit and verify that security.").

[44] White House Release, *supra*.

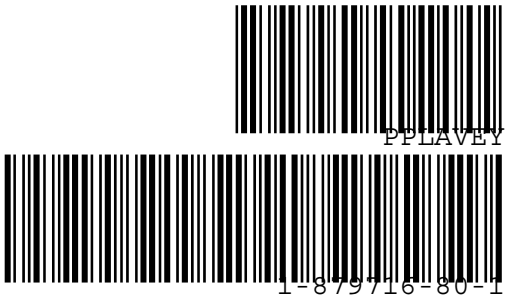
[45] See Written Statement of FCC Chairman Kevin J. Martin Before the Senate Committee on Commerce, Science & Transportation at 2 (Feb. 1, 2007) (available at hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270192A1.pdf).

[46] See, e.g., *Universal Service Contribution Methodology*, FCC 06-94, at para. 37 (2006) (available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-94A1.pdf) (extending universal service contributions to interconnected voice over Internet Protocol providers is supported by the FCC's principle of competitive neutrality).

develop a globalized, deregulated telecom industry free from national barriers and distinctions. This disparity may also reflect national security vulnerabilities in U.S.-owned providers that should be addressed through industry-wide legislation, regulations or other standards. Finally, some regulators' pursuit of merger-specific conditions reflecting labor opposition to offshore outsourcing imposes anticompetitive restrictions on the target companies and burdens on their customers. Again, legislation and agency rulemakings should address these issues in an industry-wide manner.

Acronyms

CFIUS	Committee on Foreign Investment in the United States
CS	communications sector
CWA	Communications Workers of America
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
NISP	National Industrial Security Program
NRC	Nuclear Regulatory Commission
TELPRI	Telecomunicaciones de Puerto Rico, Inc.
TSA	Transportation Security Administration


PPLAVEY
1-879716-80-1