JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW
is published semi-annually by the
Journal on Telecommunications & High Technology Law,
Campus Box 401, Boulder, CO 80309-0401

ISSN: 1543-8899

POSTMASTER: Please send address changes to JTHTL,
Campus Box 401, Boulder, CO 80309-0401

Subscriptions

Domestic volume subscriptions are available for $45.00. City of Boulder subscribers please add $3.74 sales tax. Boulder County subscribers outside the City of Boulder please add $2.14 sales tax. Metro Denver subscribers outside of Boulder County please add $1.85 sales tax. Colorado subscribers outside of Metro Denver please add $1.31 sales tax.

International volume subscriptions are available for $50.00.

Inquiries concerning ongoing subscriptions or obtaining an individual issue should be directed to the attention of JTHTL Managing Editor at JTHTL@colorado.edu or by writing JTHTL Managing Editor, Campus Box 401, Boulder, CO 80309-0401.

Back issues in complete sets, volumes, or single issues may be obtained from: William S. Hein & Co., Inc., 1285 Main Street, Buffalo, NY 14209. Back issues may also be found in electronic format for all your research needs on HeinOnline http://heinonline.org/.

Manuscripts

JTHTL invites the submission of unsolicited manuscripts. Please send softcopy manuscripts to the attention of JTHTL Articles Editors at JTHTL@colorado.edu in Word or PDF formats or through ExpressO at http://law.bepress.com/expresso. Hardcopy submissions may be sent to JTHTL Articles Editors, Campus Box 401, Boulder, CO 80309-0401. Unfortunately, JTHTL cannot return manuscripts. JTHTL uses THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (18th ed. 2005) for citation format and THE CHICAGO MANUAL OF STYLE (15th ed. 2003) for a style guide.

Cite as: 6 J. ON TELECOMM. & HIGH TECH. L. __ (2007).

JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

Volume 6 *Fall 2007*

THE UNIVERSITY OF COLORADO SCHOOL OF LAW

FACULTY, 2007-08

BARBARA A. BINTLIFF, *Nicholas Rosenbaum Professor of Law and Law Library Director*. B.A., Central Washington State College; J.D., M.L.L., University of Washington.

HAROLD H. BRUFF, *Charles Inglis Thomson Professor of Law*. B.A., Williams College; J.D., Harvard University.

MAXINE BURKETT, *Associate Professor of Law*. B.A., Williams College; J.D., University of California, Berkeley.

CLIFFORD J. CALHOUN, *Professor Emeritus*. A.B., LL.B., Harvard University.

EMILY M. CALHOUN, *Professor of Law*. B.A., M.A., Texas Tech University; J.D., University of Texas.

PAUL F. CAMPOS, *Professor of Law*. A.B., M.A., J.D., University of Michigan.

DEBORAH J. CANTRELL, *Associate Professor of Law*. B.A., Smith College; M.A., University of California, Los Angeles; J.D., University of Southern California.

HOMER H. CLARK, JR., *Professor Emeritus*. A.B., LL.D., Amherst College; LL.B., LL.M., Harvard University.

RICHARD B. COLLINS, *Professor of Law and Director of the Byron R. White Center for the Study of American Constitutional Law*. B.A., Yale College; LL.B., Harvard University.

JAMES N. CORBRIDGE, JR., *Professor Emeritus*. A.B., Brown University; LL.B., Yale University.

NESTOR DAVIDSON, *Associate Professor of Law*. A.B., Harvard University; J.D., Columbia University.

TED J. FIFLIS, *Professor of Law*. B.S., Northwestern University; LL.B., Harvard University.

WAYNE M. GAZUR, *Professor of Law*. B.S., University of Wyoming; J.D., University of Colorado; LL.M., University of Denver.

DAVID H. GETCHES, *Dean and Raphael J. Moses Professor of Natural Resources Law*. A.B., Occidental College; J.D., University of Southern California.

LAKSHMAN D. GURUSWAMY, *Professor of Law*. LL.B., Sri Lanka; Ph.D., University of Durham, U.K.

MELISSA HART, *Associate Professor of Law*. B.A., Harvard-Radcliffe College; J.D., Harvard University.

DAVID S. HILL, *Professor of Law*. B.S., J.D., University of Nebraska.

CLARE HUNTINGTON, *Associate Professor of Law*. B.A., Oberlin College; J.D., Columbia University.

J. DENNIS HYNES, *Professor Emeritus*. B.A., LL.B., University of Colorado.

HOWARD C. KLEMME, *Professor Emeritus*. B.A., LL.B., University of Colorado; LL.M., Yale University.

SARAH A. KRAKOFF, *Associate Professor of Law*. B.A., Yale University; LL.B, University of California, Berkeley.

MARK J. LOEWENSTEIN, *Nicholas A. Rosenbaum Professor of Law*. A.B., J.D., University of Illinois.

DAYNA BOWEN MATTHEW, *Associate Dean for Academic Affairs and Professor*

of Law, A.B., Harvard-Radcliffe; J.D., University of Virginia.

KRISTINE H. MCCORD, *Assistant Dean for Admissions and Financial Aid*. B.S., University of North Carolina; J.D., George Mason University.

SCOTT A. MOSS, *Associate Professor of Law*. B.A., M.A., Stanford University; J.D., Harvard Law School.

CHRISTOPHER B. MUELLER, *Henry S. Lindsley Professor of Procedure and Advocacy*. A.B., Haverford College; J.D., University of California, Berkeley.

ROBERT F. NAGEL, *Ira C. Rothgerber, Jr. Professor of Constitutional Law*. B.A., Swarthmore College; J.D., Yale University.

HELEN L. NORTON, *Associate Professor of Law*. B.A., Stanford University; J.D., University of California, Berkeley.

PAUL OHM, *Associate Professor of Law*. B.S./B.A., Yale University; J.D., University of California, Los Angeles.

VERONICA PARICIO, *Assistant Dean for Career Development*. B.A., Dartmouth College.

SCOTT R. PEPPET, *Associate Professor of Law*. B.A., Cornell University; J.D., Harvard University.

COURTLAND H. PETERSON, *Nicholas Doman Professor of International Law Emeritus*. B.A., LL.B., University of Colorado; M. Comp. L., University of Chicago; Dr. Jur., University of Freiburg (Germany).

WILLIAM T. PIZZI, *Professor of Law*. A.B., Holy Cross College; M.A., University of Massachusetts; J.D., Harvard University.

CAROLYN B. RAMSEY, *Associate Professor of Law*. B.A., University of California, Irvine; A.M., Stanford University; J.D., Stanford University.

WILLIAM E. RENTFRO, *Professor Emeritus*. B.A., University of Colorado; Th.M., LL.B., University of Denver.

PIERRE J. SCHLAG, *Associate Dean for Research and Byron White Professor of Constitutional Law*. B.A., Yale University; J.D., University of California, Los Angeles.

AMY J. SCHMITZ, *Associate Professor of Law*. B.A., Drake University; J.D., University of Minnesota.

DON W. SEARS, *Professor Emeritus*. B.S., J.D., Ohio State University.

PETER N. SIMON, *Professor Emeritus*. B.S., M.D., University of Wisconsin; J.D., University of California, Berkeley.

LAURA SPITZ, *Associate Professor of Law.* B.A., University of Toronto; LL.B., University of British Columbia Faculty of Law; J.S.D., Cornell Law School.

MARK SQUILLACE, *Professor of Law and Director of the Natural Resources Law Center*. B.S., Michigan State University; J.D., University of Utah College of Law.

NORTON L. STEUBEN, *Professor Emeritus*. A.B., J.D., University of Michigan.

ARTHUR H. TRAVERS, JR., *Professor Emeritus*. B.A., Grinnell College; LL.B., Harvard University.

LORENZO A. TRUJILLO, *Assistant Dean for Students and Professional Programs and Professor Attendant Rank*, B.A., University of Colorado; M.A., University of Colorado; Ed.D., University of San Fransisco; J.D., University of Colorado.

MICHAEL J. WAGGONER, *Associate Professor of Law*. A.B., Stanford University; LL.B., Harvard University.

PHILIP J. WEISER, *Professor of Law, Associate Dean for Research, and Executive Director of the Silicon Flatirons Telecommunications*

Program. B.A., Swarthmore College; J.D., New York University.

MARIANNE WESSON, *Professor of Law and Wolf-Nichol Fellow*. A.B., Vassar College; J.D., University of Texas.

AHMED A. WHITE, *Associate Professor of Law.* B.A., Southern University and A & M College; J.D., Yale University.

CHARLES F. WILKINSON, *University's Distinguished Professor and Moses Lasky Professor of Law*. B.A., Denison University; LL.B., Stanford University.

Research and Clinical Faculty

NORMAN F. AARONSON, *Clinical Professor*, *Legal Aid and Defender Program*. A.B., Brandeis University; J.D., Boston University.

MARGARET ANN ENGLAND, *Clinical Professor*, *Legal Aid and Defender Program*. B.A., University of Michigan; J.D., University of Denver.

H. PATRICK FURMAN, *Clinical Professor, Legal Aid and Defender Program, and Director of Clinical Programs*. B.A., J.D., University of Colorado.

COLENE ROBINSON, *Clinical Professor, Juvenile and Family Law*. B.A., Valparaiso University; J.D., Loyola University School of Law, Chicago.

JILL E. TOMPKINS, *Instructor and Director of the Indian Law Clinic*. B.A., The King's College; J.D., University of Maine.

Law Library Faculty

BARBARA A. BINTLIFF, *Nicholas Rosenbaum Professor of Law and Law Library Director*. B.A., Central Washington State College; J.D., M.L.L., University of Washington.

ALICIA BRILLON, *Reference Librarian*. B.A., M.L.I.S., University of Washington; J.D., Seattle University.

GEORGIA K. BRISCOE, *Associate Director and Head of Technical Services*. B.S., Washington State University; M.A., University of San Diego; M.L.S., University of Michigan.

YUMIN JIANG, *Technical Services Librarian.* M.S., University of Illinois, Urbana-Champaign; M.A., University of Wisconsin.

SCOTT MATHESON, *Head of Public Services and Instructor.* M.L.S., University of Washington; J.D., University of Washington.

ALAN PANNELL, *Reference Librarian*. B.A. University of Oklahoma; J.D. Western New England College; M.A. University of Arizona.

KAREN SELDEN, *Catalog Librarian*. B.S., Pennsylvania State University; M.L.S., Simmons College.

JANE E. THOMPSON, *Head of Faculty Services*. B.A., University of Missouri; M.A., J.D., University of Denver.

Legal Writing and Appellate Advocacy Faculty

AL CANNER, *Legal Writing Professor*. B.A., Brandeis University; J.D., University of Colorado.

LOUISA HEINY, *Legal Writing Professor*. B.A., J.D., University of Colorado.

DEREK H. KIERNAN-JOHNSON, *Legal Writing Professor*. A.B. Princeton University; J.D., University of Michigan.

NATALIE MACK, *Legal Writing Professor*. B.S., University of South Carolina; J.D., University of Colorado.

GABRIELLE M. STAFFORD, *Legal Writing Professor*. B.A., University of

Pennsylvania; J.D., Boston University.

TODD M. STAFFORD, *Legal Writing Professor*. B.A., Southern Methodist University; J.D., Duke University.

Research Associates

J. BRAD BERNTHAL, *Research Associate, Telecommunications*. B.A., University of Kansas; J.D., University of Colorado School of Law.

KEVIN L. DORAN, *Research Fellow, Energy & Environmental Security Initiative*. B.A., Andrews University; J.D., University of Colorado.

DOUGLAS S. KENNEY, *Research Associate, Natural Resources Law Center*. B.A., University of Colorado; M.S., University of Michigan School of Natural Resources and Environment; Ph.D., Cornell University.

KATHRYN M. MUTZ, *Research Associate, Natural Resources Law Center*. B.A., University of Chicago; M.S., Utah State University; J.D., University of Colorado.

JILL VAN MATRE, *Research Associate, Silicon Flatirons Telecommunications Program*. B.S., Indiana University; J.D., University of Colorado.

Adjunct, Adjoint and Visiting Faculty

GARRY R. APPEL, *Attorney at Law, Appel & Lucas, P.C.*, *Denver, Colorado*. B.A., J.D., University of Colorado.

ROBIN D. BARNES, *Professor of Law, University of Connecticut*, *Hartford, Connecticut*. B.A., J.D., State University of New York at Buffalo; LL.M. University of Wisconsin.

THE HONORABLE MICHAEL BENDER, *Justice, Colorado Supreme Court, Denver, Colorado*. B.A., Dartmouth College; J.D., University of Colorado School of Law School.

GEORGE BRAUCHLER, *Deputy District Attorney, First Judicial District, Golden, Colorado*. B.A., J.D., University of Colorado.

STEVEN CLYMER, *Attorney at Law, ACCORD Dispute Resolution Services, Boulder, Colorado*. A.B., St. Louis University; J.D., Case Western Reserve University.

CHRISTINE A. COATES, *Attorney at Law, Boulder, Colorado*. B.A., Houston Baptist University; M.Ed., University of Houston; J.D., University of Colorado.

TOM CONNOLLY, *Chairman of the Board and CEO, Aeroturbine Energy Corporation and Partner, Connolly Rosania & Lofstedt, PC, Colorado*. B.A., Ohio State University; J.D., Ohio State University School of Law.

THE HONORABLE WILEY DANIEL, *Judge, United States District Court for the District of Colorado*. B.A., J.D., Howard University.

DANIEL N. DEASY, *Attorney at Law, George Browning & Associates, Westminster, Colorado*. B.A., J.D., University of Colorado.

MARK FENSTER, *Associate Professor of Law, University of Florida, Gainesville, Florida*. B.A., University of Virginia; M.A., University of Texas; Ph.D., University of Illinois; J.D., Yale University.

ROGER FLYNN, *Executive Director, Western Mining Action Project, Boulder, Colorado*. B.S., Lehigh University; J.D., University of Colorado.

CRAIG C. GARBY, *Partner, Rothgerber Johnson & Lyons LLP, Denver, Colorado*. B.A., University of Colorado; Graduate Research, Waseda

University, Tokyo, Japan; M.P.A., Cornell University; J.D., Stanford University.

HANNAH R. GARRY, *Former Deputy Chief of Cabinet and Legal Officer at the International Criminal Tribunal for the Former Yugoslavia, The Hague, Netherlands*. B.A., Wheaton College; M.I.A., Columbia University; J.D., University of California, Berkeley.

SCOTT E. GESSLER, *Attorney at Law, Hackstaff Gessler LLC, Denver, Colorado*. B.A., Yale University; J.D., University of Michigan; M.B.A., Northwestern University.

JASON D. HAISLMAIER, *Partner, Holme Roberts & Owen LLP, Boulder, Colorado*. B.S., Northwestern University; J.D., Franklin Pierce Law Center.

ROGER A. HANSON, *Principal, Hanson and Hunter Consulting*. Ph.D., University of Minnesota.

ANDREW HARTMAN, *Partner, Cooley Godward LLP, Broomfield, Colorado.* A.B., University of Michigan; J.D., Georgetown University.

THE HONORABLE MORRIS B. HOFFMAN, *Judge, Denver District Court, Denver, Colorado*. B.A., J.D., University of Colorado.

BETTY R. JACKSON, *Professor of Accounting, School of Business, University of Colorado, Boulder.* BBA, Southern Methodist University; M.P.A., Ph.D., University of Texas, Austin.

JOHN LEBSACK, *Shareholder, White and Steele, P.C., Denver, Colorado*. B.A., Yale University; M.S., University of Colorado; J.D., University of Denver.

CAROL B. LEHMAN, *Law Office of Carol B. Lehman, Lakewood, Colorado*. B.A., Lawrence University; M.S., University of Wisconsin; J.D., University of Colorado.

THOMAS D. LUSTIG, *Senior Staff Attorney, National Wildlife Federation, Boulder, Colorado*. A.B., Washington University; M.S., University of Michigan; J.D., University of Colorado; Ph.D., Massachusetts Institute of Technology.

JACK MILLS, *Attorney at Law, A.J. Mills, P.C., Boulder, Colorado*. BBA, LL.B., University of Oklahoma.

CHRISTOPHER NEUMANN, *Associate, Greenberg Traurig LLP, Denver, Colorado.* B.S., University of Notre Dame; J.D., Lewis & Clark Law School.

ROBERT NICHOLS, *Adjunct Professor*. B.A., Baylor University; J.D., University of Oklahoma.

THE HONORABLE NANCY E. RICE, *Justice, Colorado Supreme Court, Denver, Colorado*. B.A., Tufts University; J.D., University of Utah.

THE HONORABLE EDWARD J. RICHARDSON, *Judge, Retired, State of Florida Circuit Court*. A.S., Brevard Community College; B.S., University of Florida; J.D., Florida State University.

WAYNE STACY, *Attorney, Cooley Godward, Denver, Colorado*. B.S., Southern Methodist University, J.D., George Washington University School of Law.

NATHANIEL TRELEASE, *President, WebCredenza, Inc., Denver, Colorado*. B.S., University of Wyoming; J.D., University of Wyoming; LL.M, University of Denver.

THE HONORABLE TIMOTHY M. TYMKOVICH, *Judge, U.S. Court of Appeals for the Tenth Circuit, Denver, Colorado*. B.A., Colorado College; J.D., University of Colorado.

PAUL WASHINGTON, *President, LJS Holdings LLC, Berkeley, California*. B.S., J.D., University of California, Berkeley.

LISA WAYNE, *Attorney at Law, William Murphy & Associates, Baltimore, Maryland*. B.A., University of Colorado, J.D., Pepperdine University College of Law.

FROM THE EDITOR

This issue highlights the proceedings of the Silicon Flatirons Telecommunications Program's Seventh Anniversary Symposium, which this year focused on the next wave of innovation in digital broadband migration.[1] From the panel on network management, two articles examine the changing nature of the network neutrality debate. Professor Jerry Kang discusses how aspects of the network neutrality debate have evolved into questions about "anti-discrimination." He uncovers several surprising lessons that can be learned from comparing and contrasting race discrimination with net discrimination. Professor Howard Shelanski then analyzes unanswered questions that create risks for committing to any single solution to the network neutrality debate. He examines the policy implications that arise from these uncertainties. Three articles then follow from the panel on digital rights management ("DRM"). Professor Pamela Samuelson and Jason Schultz show that copyright owners may be harming consumers of digital products because of the lack of effective notice about their DRM restrictions. They argue that regulation is needed while simultaneously preserving the goals of protecting copyright using DRM. Professor Neil Netanel discusses issues arising for mobile phone carriers who might be tempted to create "walled gardens" in which DRM is used to lock customers into a provider's services rather than to protect against copyright infringement. Professor Mark Lemley sorts through the patchwork of safe harbor provisions intended to protect Internet intermediaries against liability for intellectual property infringement. He argues for a uniform safe harbor rule based on the trademark immunity statute.

In addition to our symposium articles, this issue presents two additional contributions. Warren Lavey examines several recent global telecommunications mergers and acquisitions, contrasting the conditions imposed for national security and labor protection reasons with congressional and federal agency efforts to deregulate the industry. His findings and analysis suggest several ways to create more coherence when the global telecommunications industry faces the tensions between

---

1. The Silicon Flatirons Telecommunications Program, The Digital Broadband Migration: The Next Wave of Innovation, http://www.silicon-flatirons.org/conferences_old/20070211nextwave.asp (last visited Nov. 1, 2007); *see also* University of Colorado at Boulder Telecommunications Program, SFTP Conference Videos, http://telecom.colorado.edu/index.php?load=content&page_id=126 (last visited Nov. 1, 2007) (offering videos of the conference proceedings).

deregulation and U.S. national security and labor concerns. Our Production Editor, Michael Beylkin, concludes this issue with an article discussing the Supreme Court decision in *eBay, Inc. v. MercExchange, L.L.C.* and its ramifications for the biotech and pharmaceutical industries.[2] He argues that the Court's equitable test for injunctive relief in patent infringement cases should not cause any fear within these industries.

I wish to thank all our authors for providing excellent articles for this issue. Articles Editors Conor Boyle, Brian Geoghegan, Scott Grayson, and Karam Saab have played critical roles in working with each of our authors to make each article the best it can be. Without their hard work and dedication, this issue would not have been possible. Production Editor Michael Beylkin then spent countless hours helping fine tune each article so that it meets the high standards we set for publication. I will never be able to adequately thank him for all that he has done. Once again, the journal is indebted to Assistant Production Editor Mike Boucher, who has volunteered significant amounts of his time to helping on all aspects of production.

Associate Editors Patrick Thiessen, Venu Menon, Mike Varco, Ed Hafer, and Joe Chen have given generously of their time to a myriad of tasks, helping out wherever we needed them. Our Note and Comment Editors Tina Amin, Scott Challinor, Gil Selinger, and Kaydee Smith, along with our Executive Editor Carin Twining, have collectively helped choose and supervise our team of Members. In addition, I wish to thank all our Members who have given so much time and energy to cite checking this issue. Thanks also to our Managing Editor, Todd Blair for his vital role in promoting the journal and coping with our finances.

Beyond our members and editors, many other people deserve endless thanks. Our Office Manager, Martha Utchenik, has always had an open door, being available to answer questions and give overall guidance to the journal production process. Brad Bernthal, Dale Hatfield, and Jill Van Matre have provided input and insight that has driven all of us to produce better work. Our alumnae deserve thanks for their encouragement and support. And of course, the continued support of the Silicon Flatirons Program Advisory Board also makes this journal possible.

Professors Paul Ohm and Phil Weiser, our faculty co-advisors, deserve heartfelt thanks. Both Paul and Phil provide critical advice and endless support to the journal's staff. They create amazing opportunities and make valuable connections for our future careers. They also provide constant intellectual stimulation, both in and out of the classroom.

---

2. eBay, Inc. v. MercExchange, L.L.C., 126 S. Ct. 1837 (2006).

Lastly, I wish to thank my family members whose support, advice, and encouragement have made this incredible learning experience possible for me.

We hope that you find the articles contained in this first issue of the sixth volume of the *Journal on Telecommunications & High Technology Law* insightful and thought provoking.

David B. Wilson
Editor-in-Chief

JOURNAL ON
TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

Volume 6 *Fall 2007*

CONTENTS

THE DIGITAL BROADBAND MIGRATION: THE NEXT WAVE OF INNOVATION

The 7th Anniversary Silicon Flatirons Telecommunications Program Symposium co-sponsored by the Journal on Telecommunications & High Technology Law

NETWORK MANAGEMENT: BEYOND THE NET NEUTRALITY DEBATE

DIGITAL RIGHTS MANAGEMENT

ARTICLE

STUDENT NOTE

RACE.NET NEUTRALITY

JERRY KANG*

INTRODUCTION

The "net neutrality" debate is undergoing a theoretical transition. Since the late 1990s, we have moved from "open access," to "end to end," to "net neutrality," and by 2007, the question seems to have transformed into "anti-discrimination."[1] To the extent that net *discrimination* frames the question, our history and experience with *race* discrimination should be cognitively salient. Although patently different subjects, these two forms of discrimination share some similarities.[2] After all, during much of this nation's history, individuals were officially provided differential carriage (e.g., on segregated railcars),[3] access (e.g., to education),[4] and interconnection on the basis of race (e.g., to marriage).[5]

Although legal commentators have spotted such similarities, they have never been thoroughly explored.[6] This essay begins that study, with

---

* Professor of Law, UCLA School of Law. Thanks to Oscar Gandy, Douglas Lichtman, and Tim Wu for helpful comments on previous drafts. Thanks also to the Hugh & Hazel Darling Law Library at UCLA School of Law and Nathaniel Ross, who provided helpful research assistance.

1. *See* Tim Wu, *Why Have a Telecommunications Law?: Anti- Discrimination Norms in Communications*, 5 J. ON TELECOMM. & HIGH TECH. L. 15 (2006); *see also* Lawrence Lessig, *Re-Marking the Progress in Frischmann*, 89 MINN. L. REV. 1031, 1042 (2005) ("The aim of those pursuing network neutrality, however, is not some imagined neutrality, but rather the elimination of certain kinds of discrimination (just as most policies favoring equality focus on rules against certain forms of discrimination).").

2. *See, e.g.*, Wu, *supra* note 1, at 38-39 ("As discussed above, common carriage law was traditionally occupied with the distinction between 'public' business, and the rest, which were presumably 'private.' The same distinction is central to the anti-discrimination regime surrounding public accommodations in the United States. As the example[] goes, if you operate a restaurant, you must serve customers of all races but you have no duty to invite the man on the street to a dinner party at your house."); Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 25 (2005) (critiquing baseline assumption of IP as "neutral" and situating it in the "broader debates about [equality] jurisprudence").

3. Plessy v. Ferguson, 163 U.S. 537 (1896), *abrogated by* Brown v. Bd. of Educ. of Topeka, 347 U.S. 483 (1954).

4. Brown v. Bd. of Educ. of Topeka, 347 U.S. 483 (1954).

5. Loving v. Virginia, 388 U.S. 1 (1967).

6. Tim Wu has done the most to further this way of thinking. *See, e.g.*, Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 150 (2003) (pointing out the value of the analogy as clarifying the distinction between

the goal of gleaning lessons for telecommunications policy.[7] Because the domains of discrimination differ radically, one expects little payoff from the comparison and contrast. I promise a modest surprise. More specifically, a comparison and contrast between race discrimination and net discrimination teaches us, first, to particularize the discrimination at issue and be wary of what I call normative carve-outs in defining discrimination. Second, the comparison sensitizes us to the clash between welfarist and deontological concerns that have not been adequately distinguished within the net neutrality debate. Third, it urges us to be cautious about facile assurances that individual, firm, or market rationality will ensure the public interest.

I. DEFINITIONS AND NORMATIVE CARVE-OUTS

In order to discuss any sort of discrimination usefully, we must first define it. Let's start with a simple, narrow, and abstract definition: discrimination is the differential treatment of some entity X, based on that entity's supposed or actual attribute Y.

In the race context, X is typically a human being and Y is that person's race. Immediately, various complications arise. For example, with regards to X, we sometimes are concerned with *groups* of human beings or *entities* that are themselves not human (e.g. a church), but are nonetheless associated with racialized human beings (e.g., a predominantly Korean immigrant congregation). With regards to Y, complications include the fact that "race" is often used as a placeholder for related attributes, such as national origin, ethnicity, or color. Indeed, race itself has no uncontroversial definition from, say, scientific or medical practice. Instead, as the saying goes, race is a social construction, by which I mean to emphasize that the various racial categories and the rules by which we map human bodies into those categories have been created by society, as a function of history, culture, politics, and ideology.[8]

When I say that X (a human being) is treated differently "based on" some attribute Y (race), I mean that race is a "but for" cause of the differential treatment. In social cognition terms, the racial attribute triggers stereotypes and attitudes associated with that racial category, which alter interpersonal interactions and evaluations of the individual

---

"justified and suspect bases of discrimination").

7. For an inquiry in the other direction — trying to glean lessons for race policy from telecommunications — see Brant T. Lee, *The Network Economic Effects of Whiteness*, 53 AM. U. L. REV. 1259 (2004). Lee's focus is not on the network neutrality debate, but he draws insights from network economics to parse race relations.

8. For a fuller discussion of this racial mechanics model, see Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131, 1138-47 (2000) [hereinafter Kang, *Cyber-Race*].

mapped to that category.[9] Examples of traditional race discrimination are well-known. Recall the examples of *Plessy*, *Brown*, and *Loving*.[10] Some modern cases are more subtle or contested. For example, White students sometimes complain that affirmative action makes them the new victims of discrimination. This is Grutter's lament.[11]

In the net context, X can be data (e.g., packet or stream), application service, hardware (e.g., consumer premises equipment), or some transport infrastructure.[12] Y can be any attribute associated with these entities, such as semantic content, digital rights management status, identities of communicating parties, type of application service, hardware manufacturer, and so on. Examples of network discrimination are also well known. One reason why AT&T was divested in the 1980s was that it provided discriminatory interconnection between its local exchanges and competing long distance providers, such as MCI.[13] There are more modern examples. For example, the Federal Communications Commission fined Madison River, a telco broadband provider, $15,000 for blocking ports necessary to use Voice over Internet Protocol ("VoIP").[14] Just recently, AT&T announced that it will scan for and not transport any content that it deems to violate intellectual property laws.[15]

Notice that race discrimination and net discrimination, as I have used these terms, differ in their level of generality. When discussing race discrimination, we have been talking about the differential treatment of individuals based on a single attribute: race. We have ignored other attributes, such as gender, looks, intelligence, lineage, and so on. By contrast, in our definition of net discrimination, we selected neither a single X (entity) nor a single Y (attribute). In other words, net discrimination has not been particularized. At one extreme, it might raise a troubling question of viewpoint discrimination against unpopular content (e.g., a broadband provider blocking access to Arabic sites that stream videos of American troops shot by snipers in Iraq).[16] At the other

---

9. *See* Jerry Kang, *Trojan Horses of Race*, 118 HARV. L. REV. 1489, 1499-1504 (2005) [hereinafter Kang, *Trojan Horses*]; *see also* Jerry Kang & Mahzarin R. Banaji, *Fair Measures: A Behavioral Realist Revision of "Affirmative Action"*, 94 CAL. L. REV. 1063, 1083-85 (2006).

10. *See supra* notes 3-5.

11. Grutter v. Bollinger, 539 U.S. 306 (2003).

12. *See* Tim Wu, *The Broadband Debate, A User's Guide*, 3 J. ON TELECOMM. & HIGH TECH. L. 69, 73 (2004) (referring to discrimination on the basis of "uses, users, or content" and also quoting FCC Commissioner Michael Copps as discussing anti-discrimination against "users, ideas, and technologies").

13. For a general discussion of AT&T's breakup, see JERRY KANG, COMMUNICATIONS LAW AND POLICY: CASES AND MATERIALS 535-59 (2d ed. 2005).

14. *See* Madison River Commc'ns, LLC, *Order*, 20 FCC Rcd. 4295, 4296-97 (2005), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf.

15. James S. Granelli, *AT&T to Target Pirated Content; It Joins Hollywood in Trying to Keep Bootleg Material Off Its Network*, L.A. TIMES, June 13, 2007, at C1.

16. Google seems to be doing precisely this on YouTube. Google has officially stated

extreme, it might refer to a mundane question of subscription status discrimination (e.g., a broadband provider not connecting a user to its wireless network because the user is not a paying subscriber). We are concerned more about the former than the latter, just as we might be more concerned about discrimination in law firm promotion based on race than on billable hours. The lesson here is to avoid confusion by specifying the X and Y in any net discrimination conversation.

What lessons can be drawn from a comparison between discrimination in both domains, race and net? First, we immediately notice how the definition of discrimination is sharply contested. In the race context, many "structuralists" would object to the narrow definition of discrimination I presented. For instance, a requirement of differential treatment of persons based on their race may not capture pure disparate impact cases. Interestingly, in the net context, various commentators have made similar structuralist arguments about the current Internet Protocol, which delivers packets on a best-efforts basis without quality of service ("QoS") guarantees. This architecture is not neutral; instead, it discriminates against those services that require just such assurances.[17] Again, no differential treatment of some packet is necessary for there to be a colorable claim of "discrimination" as that word is reasonably used.

Having stated the obvious — that discrimination is hard to define[18] — let me focus on a single facet of this problem. In the race context, because the word "discrimination" has negative valence, there is a tendency to carve out normatively acceptable treatment from the term's very definition. In other words, if some practice of differential treatment is "good," then people shy away from calling it "discrimination." Claims of normative acceptability typically point to: (i) some benign nature as gauged by purposes, effects, or social meanings; (ii) some rational cost-benefit analysis based on accurate probabilities; or (iii) some public/private distinction, in which private matters are insulated from ethical critique and legal intervention. To give examples, (i) affirmative action programs are said not to count as discrimination because of their benign nature; (ii) terrorist profiling is defended as not discrimination because of its claimed probabilistic rationality; and (iii) how we choose

---

that it removed sniper videos that "display graphic depictions of violence *in addition to any war footage (U.S. or other) displayed with intent to shock* or disgust, *or graphic war footage with implied death* (of U.S. troops or otherwise)." Edward Wyatt, *Anti-U.S. Attack Videos Spread on Web*, N.Y. TIMES, Oct. 6, 2006 (emphasis added).

17. *See* Wu, *supra* note 6, at 148 (pointing out how the internet protocol "implicitly disfavors"); *id.* at 142 (making the same observation and calling it "favoritism"); Yoo, *supra* note 2, at 25 (pointing out "nonneutrality inherent in the choice of baseline principles" and referencing Herbert Wechsler's "neutral principles" article).

18. *See, e.g.*, Barbara A. Cherry, *Misusing Network Neutrality to Eliminate Common Carriage Threatens Free Speech and the Postal System*, 33 N. KY. L. REV. 483, 485-87 (2006) (comparing various definitions and framings of net neutrality debate).

marriage partners is suggested to be sufficiently private such that the question of discrimination is simply off point.

In the net context, we see similar attempts at normative carve-outs from the definition of "discrimination." Interestingly, they too sound in terms of (i) benign natures, (ii) rational justifications, and (iii) public/private distinctions. Stopping spam or hacking, it is argued, should not be derogated as discrimination because of the benign purpose.[19] Allowing price discrimination, especially when costs are in fact different, is defended as economically rational and thus should not be stigmatized as discrimination.[20] Finally, private networks should be able to do what they will with their property, without any complaints of discrimination.[21]

In defining net discrimination, should we allow such normative carve-outs? Our experience with race discrimination analysis suggests no. Instead "discrimination" should be defined neutrally, to describe solely the behavior or act of treating differently some entity X on the basis of some attribute Y. Whether that behavior is socially, ethically, or legally warranted is a critical question, but one that should be asked subsequently.

This distinction between the *fact* of discrimination and its *value* helps clarify the analysis. First, it avoids arguments by definitional assertion. When someone responds "by definition, that's not discrimination!" the other side is rarely persuaded since the thrust of the complaint has been side-stepped, not met head-on. Simply recall any shouting match between those who promote and those who resent race-based affirmative action, or those who promote and those who resent race-based profiling. Second, avoiding normative carve-outs allows grouping in one place all the arguments about the propriety of any discrimination. Otherwise, these considerations surface twice – initially at the definitional stage and later in considering whether some special set

---

19. *Cf.* Adam D. Thierer, *"Net Neutrality": Digital Discrimination or Regulatory Gamesmanship in Cyberspace?*, 507 POL'Y ANALYSIS (Cato Inst., D.C.), Jan. 12, 2004, at 8-13 (identifying "Rational Reasons for Discrimination"), *available at* http://www.cato.org/pubs/pas/pa507.pdf.

20. Alfred E. Kahn, *Telecommunications: The Transition from Regulation to Antitrust*, 5 J. ON TELECOMM. & HIGH TECH. L. 159, 177-78 (2006) ("The opposition to 'tiering' as such – extra charges for 'access to the express lane' . . . is economically ignorant. The costs – both short-run (the opportunity costs of giving priority to the higher-speed uses) and long-run (the costs of the investments to provide additional broadband capacity, to relieve that congestion) – are, presumably, higher for the users requiring the 'express lane.' It is therefore *not discriminatory* for those costs to be levied on the services requiring their incurrence. . . ." (emphasis added)).

21. *See* Eli M. Noam, *Beyond Liberalization II: The Impending Doom of Common Carriage*, 18 TELECOMM. POL'Y 435, 452 (1994) (suggesting that network owners be forced to be either private or public, and if they choose private, to have plenary power over their private zones).

of circumstances overcomes the presumption against discrimination (e.g., to achieve a compelling interest through narrowly tailored means). The point of avoiding normative carve-outs is to promote analytical clarity, crucial to good policy analysis.[22]

In sum, the general point is that "discrimination" is difficult to define. Accordingly, we must always specify the particular net discrimination at issue, which specific X (the object of differential treatment) and which specific Y (the entity's attribute) are at issue. Although obvious, this caution bears repeating, especially because strawpersons are tempting.[23] Finally, we should avoid normative carve-outs from the definition of discrimination, at least during the policy analysis phase. If the discrimination should be legally tolerated, indeed economically encouraged, that case should be made not at the point of threshold definition, but *later* in the analytical process.

II. INCOMMENSURABLE HARMS

Later starts now. What's actually wrong with discrimination? If the professional philosophers will indulge me, I suggest that the reasons against discrimination can be roughly divided into two categories: deontological and welfarist. By "deontological," I mean reasons based on some moral duty or obligation that is not principally determined by some consequentialist calculation. These arguments tend to sound in terms of equality, justice, and fairness. By contrast, "welfarist"

---

22. I recognize that in drafting legislation or regulation, clarity may not be the sole or principal purpose. That said, certain bills are drafted consistently with this analytical structure; they prohibit discrimination defined in some general manner, and later in a subsection, carve out particular discriminations that shall not be deemed as such. For example, a bill titled the "Internet Freedom and Nondiscrimination Act of 2006" reads:

> (a) It shall be unlawful for any broadband network provider . . .
>
> (c) Nothing in this section shall be construed to prevent a broadband network provider from taking reasonable and nondiscriminatory measures—
>
> (1) to manage the functioning of its network, on a systemwide basis, provided that any such management function does not result in discrimination between content, applications, or services offered by the provider and unaffiliated provider;
>
> (2) to give priority to emergency communications . . . .

H.R. Res. 5417, 109th Cong. §3 (2006) (proposing to insert a section into the Clayton Act on "DISCRIMINATION BY BROADBAND NETWORK PROVIDERS"); *see also* Internet Non-Discrimination Act of 2006, S. Res. 2360, 109th Cong. §4(b) (2006), which states:

> (1) may–
>
> (A) take reasonable and non-discriminatory measures to protect subscribers from adware, spyware, malware, viruses, spam, pornography, content deemed inappropriate for minors, or any other similarly nefarious application or service that harms the Internet experience of subscribers, if such subscribers . . . .

23. *See, e.g.*, Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. ON TELECOMM. & HIGH TECH. L. 329, 333-34 (2007) (noting how opponents of "net neutrality" often adopt broader definitions as strawperson).

arguments emphasize net benefits and costs as measured by some metric of social welfare. They are principally consequentialist, have philosophical affinities with utilitarianism, and tend to focus on efficiency.

In the race context, as between deontological versus welfarist arguments, the former predominate. To be sure, various arguments emphasize welfare losses and gains. For example, racial diversity in the corporate boardroom is sometimes defended as generating better firm decisions. Prominently, the Supreme Court has also found that diversity improves learning, which is praised as a compelling interest — at least in higher education.[24] Still, such welfarist arguments constitute merely the tail of the dog. What makes race discrimination so emotionally and politically charged is that it alleges some deontological error, a violation of some moral imperative (whether it be treating human beings as equals or remaining steadfastly colorblind in state action), not some mere spreadsheet error.

By contrast, in the net context, welfarist arguments dominate. As Wu notes, nearly all sides of the debate seem to agree that the goal of "network neutrality" policymaking is to maximize innovation, which is well understood in welfarist terms.[25] Understanding the Internet as an infrastructural good also emphasizes efficiency concerns.[26] It is this predominance of welfarist concerns that make plausible Robert Hahn and Robert Litan's contention that although nondiscrimination has "superficial appeal," it should be rejected on efficiency grounds.[27] The *appeal*, I gather, draws on a family resemblance with the deontological imperatives against better-known forms of discrimination, such as those outlawed by Title VII of the Civil Rights Act. It is *superficial*, however, in their view because in net discrimination, welfarist arguments should be privileged over deontological ones.[28] Economist Alfred Kahn similarly suggests that deontological concerns are "social goals" that should be the subject of "extra-market, political determination."[29] In

---

24. *See Grutter*, 539 U.S. at 322. *But cf*. Parents Involved in Cmty. Sch. v. Seattle Sch. Dist. No. 1, 127 S. Ct. 2738, 2753-54 (2007).

25. *See* Wu, *supra* note 1, at 26.

26. *See* Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 922 n.12 (2005) (identifying normative commitment as "maximizing social welfare"); Wu, *supra* note 12, at 72-73 (discussing "infrastructure principle" as one of three prescriptive principles of Openist's position).

27. Robert W. Hahn & Robert E. Litan, *The Myth of Network Neutrality and the Threat to Internet Innovation*, 2007 MILKEN INST. REV., at 33, *available at* http://aei-brookings.org/admin/authorpdfs/page.php?id=1342.

28. *Cf. Net Neutrality: Hearing Before the S. Comm. On Commerce, Sci. & Transp.*, 109th Cong. 61-62 (2006) (testimony of J. Gregory Sidak, Visiting Professor at Law, Georgetown University Law Center), *available at* http://commerce.senate.gov/public/_files/30115.PDF.

29. Kahn, *supra* note 20, at 176 ("But either that is exactly what it is or should be about

starker terms, he contends that network neutrality proponents are "talking either nonsense or the – prosaic – prose of competition and monopoly," which are problems within the welfarist category for which exist "reasonable, non-ideological resolutions."[30]

Still, in the net context, as Bill Herman has recently argued, there is something else going on.[31] In my terminology, it is deontic, and it is not nonsense.[32] We find it in the literature of the various grass roots consumer organizations engaging the issue. For example, the "Save the Internet" FAQ states: "Net Neutrality is the reason why the Internet has driven economic innovation, *democratic participation, and free speech online*. . . . On the Internet, *consumers are in ultimate control* — deciding between content, applications and services available anywhere, no matter who owns the network."[33]

Non-welfarist concerns also appear in proposed findings of draft legislation, as in the Net Neutrality Act of 2006: "Because of the vital role that broadband networks and the Internet play for America's economic growth *and our First Amendment rights* to speak, the United States should adopt a clear policy endorsing the *open nature of Internet communications and freely accessible* broadband networks."[34]

Of course, these more political and distributive justice anxieties can be shoehorned into welfarist lingo, but the fit is awkward. My point here

---

or — their rhetoric of 'monopoly' and 'discriminations' and squeezes notwithstanding — the [net neutrality] advocates are really talking about social goals that cannot be achieved by a market economy, however perfectly functioning — uses of resources and distributions of income in their opinion properly subject to extra-market, political determination.").

30. *Id.* at 188; *see also* Bruce M. Owen, *The Net Neutrality Debate: 25 Years after United States v. AT&T and 120 Years After the Act to Regulate Commerce*, PERSP. FROM FSF SCHOLARS (Free State Found., Potomac, Md.), Feb. 20, 2007, at 3-4 (complaining that network neutrality advocates are vague and lack analytical rigor, then quickly translating the debate into a vertical integration economics problem). In the course of his argument, Owen suggests that the original decision to break up AT&T and create a "stark and permanent isolation of the monopoly local service companies from participation in any competitive business requiring use of their monopoly facilities" may well have been a good idea. *Id.* at 6-7. Surely net neutrality advocates would be comfortable doing the same with all wireline broadband Internet service providers.

31. *See* Bill D. Herman, *Opening Bottlenecks: On Behalf of Mandated Network Neutrality*, 59 FED. COMM. L.J. 103, 116 (2006) (explicitly distinguishing the value of innovation from the value of media diversity, which is promoted by a neutral network that does not discriminate based on content).

32. For gestures in this vein, see*, e.g.*, Mark Cooper, *Open Access to the Broadband Internet: Technical and Economic Discrimination in Closed, Proprietary Networks*, 71 U. COLO. L. REV. 1011, 1012 (2000) ("We should understand that we are part of a worldwide political battle; that we have views about what rights should be guaranteed to all humans, regardless of their nationality; and that we should be ready to press those views in this new political space opened up by the Net.").

33. Save the Internet, Frequently Asked Questions, http://www.savetheinternet.com/=faq (emphasis added) (last visited Sept. 23, 2007).

34. H.R. Res. 5273, 109th Cong. § 2(13) (2006) (emphasis added).

is not that this translation is impossible; rather, it is simply to spotlight the fact that welfare contests are not all that's going on.

Suppose we take such deontic anxieties at face value.[35] These concerns are not solely about efficient pricing and dead-weight loss, but also about the basic distribution of communicative power and opportunities among private actors. The concern is that broadband pipe owners will subtly manipulate the content that flows through their bottlenecks, at least in pathological cases.[36] In other words, even though broadband Internet providers generally look and feel like common carriers who dutifully deliver packets from here to there with little regard to who sent the packets and what they mean, they aren't actually common carriers. Even though your traditional "phone company" may be providing the fast Internet connection over the high frequency portion of the same twisted pair copper line that provides traditional telephone service, they are not actually providing "telecommunications services" regulated under Title II of the Communications Act. Rather, they are providing "information services" subject to far weaker requirements of Title I.[37]

In this way, the serious anxieties expressed about mass media consolidation resurface in the net neutrality debate.[38] It is all of one piece. As fewer and fewer entities own more and more media properties, they invite the public to relax and to enjoy the benefits of improved efficiencies. Media owners promise never to exercise any sort of spin because they are just satisfying market demand, and if they do anything untoward, fierce competition would instantly discipline misbehavior.

The public, however, remains skeptical. Ownership does influence content. Rupert Murdoch's ownership of FOX alters what is broadcast on FOX.[39] Even the free-market oriented reporters of the Wall Street Journal recognize that this is so, at least when their own jobs and autonomy are at stake.[40] This may not entirely be a bad thing; indeed,

---

35. My colleague Doug Lichtman reminds me that findings of fact in draft legislation may reveal as much about the strength of particular interest groups and focus group politics than anything especially deontic or public-interest minded.

36. Vincent Blasi has written astutely about the virtues of adopting a pathological perspective in interpreting the First Amendment. *See* Vincent Blasi, *The Pathological Perspective and the First Amendmen*t, 85 COLUM. L. REV. 449 (1985).

37. *See* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Report & Order & Notice of Proposed Rule Making*, 20 FCC Rcd. 14,853 (2005).

38. For insightful discussion of the relationship between mass media ownership and self-governance, see C. EDWIN BAKER, MEDIA CONCENTRATION AND DEMOCRACY: WHY OWNERSHIP MATTERS (2006).

39. *See* C. Edwin Baker, *Media Structure, Ownership Policy, and the First Amendment*, 78 S. CAL. L. REV. 733, 736 (2005) (discussing the "Berlusconi effect").

40. So do the free-market minded Wall Street Journal reporters who boycotted their jobs for half a day in protest. Posting of Jim Romenesko to Poynter Online, http://poynter.org/forum/view_post.asp?id=12696 (June 28, 2007).

the FCC has suggested that this is precisely what diversity of ownership should entail.[41] But it is facile to suggest that ownership is entirely irrelevant. To provide just one example, Cumulus Media Inc. stopped playing the Dixie Chicks when they criticized the sitting President for starting the Iraq war.[42] It was also ownership that prompted the broadcast networks to remain silent about the digital TV spectrum that was given *gratis* to current television broadcast licensees, *sans* billions of dollars in auction payments.[43]

Further, such deontic concerns are not recent inventions — they have been around for a long time, even before the Internet. To give just one example, in the Modified Final Judgment, Judge Harold Greene specifically barred AT&T from the nascent "electronic publishing" industry for at least seven years. Electronic publishing was defined as: "the provision of any information which a provider or publisher has, or has caused to be originated, authored, compiled, collected, or edited, or in which he has a direct or indirect financial or proprietary interest, and which is disseminated to an unaffiliated person through some electronic means."[44]

Among other things, Judge Greene feared that AT&T would discriminate against other e-publishers by giving priority traffic to its own publishing operations, collecting and analyzing intelligence about competitors gleaned from transactional data, and providing second-class maintenance to a time sensitive enterprise. These arguments were not strictly economic. Instead, Judge Greene continued:

> Beyond [these competitive considerations], AT&T's entry into the electronic publishing market poses a substantial danger to First Amendment values.
>
> The goal of the First Amendment is to achieve 'the widest possible dissemination of information from diverse and antagonistic sources.' *Associated Press v. United States*, 326 U.S. 1, 20 (1945). This interest in diversity has been recognized time and again by various courts. *Red Lion Broadcasting Co. v. F.C.C.*, 395 U.S. 367, 390 (1969). . . .
>
> . . . .
>
> . . . The Federal Communications Commission is charged by the

41. *See* 2002 Biennial Regulatory Review, *Report & Order & Notice of Proposed Rule Making*, 18 FCC Rcd. 13,620 (2003).

42. *See* Geoff Boucher, *Fans Not Buying Chicks' Apology*, L.A. TIMES, Mar. 19, 2003, at E4.

43. *See* KANG, *supra* note 13, at 645 (describing DTV coverage).

44. United States v. Am. Tel. & Tel. Co., 552 F. Supp. 131, 181 (D.D.C. 1982).

> Communications Act with granting broadcast licenses in the 'public interest, convenience and necessity.' . . .
>
> . . . .
>
> Certainly, the Court does not here sit to decide on the allocation of broadcast licenses. Yet, like the FCC, it is called upon to make a judgment with respect to the public interest and, like the FCC, it must make that decision with respect to a regulated industry and a regulated company.
>
> In determining whether the proposed decree is in the public interest, the Court must take into account the decree's effects on other public policies, such as the First Amendment principle of diversity in dissemination of information to the American public. . . .
>
> . . . .
>
> Applying this diversity principle to the issue here under discussion, it is clear that permitting AT&T to become an electronic publisher will not further the public interest.[45]

My point here is not to persuade readers that Judge Greene was right or wrong. Instead, it is simply to observe that matters beyond efficiency — in this case, phrased in terms of First Amendment rights-talk — mattered in the breakup of AT&T, which was, after all, a common carrier. And surely something similar is going on today with the net neutrality debate.

Having made this deontological versus welfarist distinction, what is the payoff of the race versus net discrimination comparison? First, attention to race discrimination sensitizes us to the existence of deontological objections even in the net discrimination debate.[46] And this sensitivity has policy consequences. For example, Christopher Yoo argues that even if every broadband provider were structurally quarantined out of adjacent markets, there would be no reduction in market power. "Vertical disintegration . . . has no effect on last-mile providers' ability to extract supracompetitive returns. Consumers will receive benefits only by promoting entry by alternative network capacity."[47] Even if this is right, it focuses solely on welfarist concerns

45. *Id*. at 183-84 (citations omitted).

46. Baker suggests that increased sensitization is necessary because many economics-minded analysts have a tin ear to noncommodified concerns. *See* Baker, *supra* note 39, at 742-44.

47. Yoo, *supra* note 2, at 16.

about monthly broadband bills charged to consumers. The deontological concern — that private firms will leverage their ownership of broadband pipes to control the content traveling through those pipes — is far better satisfied by the quarantine.

Second, and tightly related, we can better appreciate that the hardest questions arise from clashes *across* the deontological-welfarist boundary. To be sure, hard questions surface within each category. For instance, within the welfarist category, there are difficult empirical questions in the race discrimination debate. Does affirmative action in admissions provide net welfare benefits or losses, however measured? Similarly, within the net discrimination debate, which legal arrangements will maximize social welfare by simultaneously encouraging innovation without undermining capital investment?[48] After all, not everyone emphasizes the marvelous innovations at network's edge;[49] others bet on the center.[50]

However difficult these intra-category questions are, even harder questions come from the incommensurability between deontological and welfarist arguments.[51] In the race context, for instance, how shall we compare a deontological complaint (for example, you should not intern me simply because I am ethnically Japanese) against a welfarist justification (we must intern you because our military leaders have concluded that your kind constitute a military threat of espionage and sabotage)?[52] The same goes within the net context. Suppose that there is some welfarist justification for not opening access to cable broadband pipes based on vertical integration efficiencies. Many will still complain that such economic analysis does not meet their fundamental concern, namely that some private corporation that provides what "looks and

48. *See generally* van Schewick, *supra* note 23, at 383-89 (discussing benefits, costs, and trade-offs on innovation and welfare).

49. For an example of someone who does see innovations coming from the edge, see Wu, *supra* note 1, at 37-38 ("The strongest track record of innovation comes from the network edges, not the center.").

50. *See*, *e.g.*, BRUCE M. OWEN & GREGORY L. ROSSTON, AEI-BROOKINGS JOINT CTR. FOR REGULATORY STUDIES, LOCAL BROADBAND ACCESS: *PRIMUM NON NOCERE* OR *PRIMUM PROCESSI?* A PROPERTY RIGHTS APPROACH 28-29 (2003), *available at* http://www.aei.brookings.org/admin/authorpdfs/page.php?id=285.

51. *Cf.* Oscar H. Gandy, Jr., *Quixotics Unite! Engaging the Pragmatists on Rational Discrimination*, *in* THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND 318, 321 (David Lyon ed., 2006) (suggesting special difficulty of trying to maximize incompatible outcomes when evaluating on "historically distinct, if not orthogonal criteria, such as efficiency and equality").

52. *See generally* ERIC K. YAMAMOTO, MARGARET CHON, CAROL L. IZUMI, JERRY KANG & FRANK H. WU, RACE, RIGHTS AND REPARATION: LAW AND THE JAPANESE AMERICAN INTERNMENT (2001); Jerry Kang, *Denying Prejudice: Internment, Redress, and Denial*, 51 UCLA L. REV. 933 (2004); Jerry Kang, *Thinking through Internment: 12/7 and 9/11*, 9 ASIAN L.J. 195 (2002).

feels" like a transportation service — often the descendents of legal monopolies, with all the benefits of first mover advantage, exploiting public rights-of-way — should not be able to exercise even limited influence over the content or applications that flow through those pipes. The implicit argument here is that some (admittedly inchoate) right to access information without private influence is being infringed, not that some utility function is inadequately maximized.

At this point, the predictable response is to suggest that these deontological concerns are woolly-headed and bleeding-hearted, and that in the net context, we should focus only on welfarist concerns.[53] But precisely the same thing can be said and has been said of many forms of race discrimination. Those who fancy themselves as Bayesian discriminators proudly assert that they are acting on the basis of evidence-based stereotypes (generalizations about social categories) that are justified by accurate assessments of base rate probabilities. It is not "efficient," they exclaim, to screen White, Christian grandmothers for bombs at airports; rather, we should focus on swarthy skinned, young Muslim males. It is not "efficient" for me as a restaurant server to give top-notch service to a Black customer because they do not tip as well, and here are the statistical data to demonstrate that.[54] It is rational for me to compliment people with last names such as Wu, Yoo, Ohm, and Kang on their English because Asians in America are majority immigrants, and if they are offended, they are being too sensitive. And so on. If someone objects to this kind of thinking, why shouldn't the same response be made? Stop being woolly-headed and bleeding-hearted! My guess is that there would at least be a pause. And rightly so.[55]

Let me be clear: I am not equating exclusively welfarist analyses of net neutrality to statistical racial discrimination. That said, one must argue for — not simply assert — the position that net discrimination must be understood exclusively in welfarist terms.

In sum, race discrimination sensitizes us to two different categories of arguments against discrimination that exist even in the net context: deontological and welfarist. Within each category, the analysis is difficult on both theoretical and empirical grounds. However, still more perplexing is an inter-category comparison *across* the deontological and

---

53. This argument has been made in even more strident terms—namely, that welfare should always trump fairness. *See* LOUIS KAPLOW & STEVEN SHAVELL, FAIRNESS VERSUS WELFARE (2002). For a devastating critique, see Jules L. Coleman, *The Grounds of Welfare*, 112 YALE L.J. 1511 (2003) (reviewing LOUIS KAPLOW & STEVEN SHAVELL, FAIRNESS VERSUS WELFARE (2002)).

54. *Cf.* Ian Ayres et al., *To Insure Prejudice: Racial Disparities in Taxicab Tipping*, 114 YALE L.J. 1613, 1630 tbl.6 (2005).

55. *See generally* Gandy, *supra* note 51, at 323-31 (summarizing arguments raising concerns about various forms of racial statistical profiling).

welfarist boundary. The net discrimination debate also suffers from this difficulty. Although welfarist arguments predominate, there is a deontological vein of thinking that must be addressed, and on its own terms. The deontological concerns are neither paranoid nor nonsensical, and welfarist assurances do not lift deontological dread.

III. RATIONALITY'S CONSTRAINTS

Many Americans believe that race discrimination is largely a problem of the distant past. Many believe that we have learned from our mistakes and that we are now a far more rational people and economy, driven by a hard-nosed and practical reason. This position is supported by a loose syllogism. We are rational; race discrimination is irrational; therefore, we must not be engaging in race discrimination. An addendum to this syllogism is that anything that looks like "discrimination" that is in fact rational should not be called discrimination in the first place.[56] This is the normative carve-out discussed above.

Does this argument get the facts right? To start off, are we in fact rational? "Rational" in the above syllogism roughly means instrumental rationality. An individual behaves rationally to the extent that her actions help satisfy her preferences and achieve her chosen goals. Individuals do not, however, behave completely rationally. The heuristics and biases literature has cataloged a laundry list of cognitive errors.[57] Hedonic psychology reveals that we do not know very well what will make us happy.[58] Still more interesting is the recent work in implicit social cognition, which describes how mental associations that operate automatically and not necessarily with any self-awareness or self-reflective endorsement can nevertheless alter our behavior.[59] As evidence of these various implicit biases and their predictive validity

---

56. *See, e.g.*, Thierer, *supra* note 19, at 6 ("[S]ometimes discrimination really isn't discrimination at all. More specifically, what one party considers discrimination may be judged by others to be perfectly sensible or justifiable behavior.").

57. *See, e.g.*, Russell B. Korobkin & Thomas S. Ulen, *Law And Behavioral Science: Removing The Rationality Assumption From Law And Economics*, 88 CAL. L. REV. 1051 (2000); Donald C. Langevoort, *Behavioral Theories of Judgment and Decision Making in Legal Scholarship: A Literature Review*, 51 VAND. L. REV. 1499 (1998).

58. *See generally* DANIEL GILBERT, STUMBLING ON HAPPINESS (2006); Samuel R. Bagenstos & Margo Schlanger, *Hedonic Damages, Hedonic Adaptation, and Disability*, 60 VAND. L. REV. 745 (2007).

59. *See generally* Kang, *Trojan Horses*, *supra* note 9; Kang & Banaji, *supra* note 9. For succinct summaries of the science, see Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 CAL. L. REV. 945, 954-58 (2006); Kristin A. Lane, Jerry Kang, & Mahzarin R. Banaji, *Implicit Social Cognition and Law*, 3 ANN. REV. L. & SOC. SCI. (forthcoming 2007). For an introduction to social cognition and the way it affects legal scholarship, see Ronald Chen & Jon Hanson, *Categorically Biased: The Influence of Knowledge Structures on Law and Legal Theory*, 77 S. CAL. L. REV. 1103 (2004).

increase, we have more reason to question the rationality presumption. We may not be treating people in a colorblind fashion notwithstanding our explicit and sometimes righteous endorsement of that moral principle.

Even if individuals are not entirely rational, perhaps markets do much better. Indeed, an illustrious line of economic thinking suggests that race discrimination is inefficient and therefore cannot survive in a competitive market.[60] If a racist firm inappropriately discounts the value of a human resource on the basis of an irrelevant attribute, such as race, then other non-racist firms will price the human asset correctly and simply out-compete. The inevitable result is that race discrimination will be burned away.

Again, this account gets things descriptively wrong. First, the market may simply satisfy a "taste" for discrimination held by consumers. If a client feels subtly more confident having a White male attorney over an Asian female attorney as the lead lawyer for mission-critical litigation, then an unhindered market will just as subtly satisfy that request. Second, such preferences may produce self-fulfilling prophecies in the form of positive feedback loops that cause underinvestment in human capital[61] and potentially disrupt performance on ability tests.[62] Third, even if certain competitive firms recognize this phenomenon and want to exploit it for competitive gain, there would be a collective action problem in dismantling the feedback loop because a single firm cannot alter the general incentive structures created by the general marketplace.[63]

To be fair, no one makes the unqualified claim that individuals always, without exception, behave rationally. And no one suggests that markets are perfect disciplinarians. So, the real debate is about how often and in what contexts do individuals and markets behave "rationally" in contexts where race matters. My only point here is that we have good reasons to be cautious of any robust rationality

---

60. *See*, *e.g.*, GARY S. BECKER, THE ECONOMICS OF DISCRIMINATION (2d ed. 1971). The most prominent modern proponent of this view is Richard Epstein, though Epstein posits not that a competitive market will necessarily eradicate discrimination, but rather that any discrimination which survives in such a market must be rational and therefore have useful social consequences. *See* RICHARD EPSTEIN, FORBIDDEN GROUNDS: THE CASE AGAINST EMPLOYMENT DISCRIMINATION LAWS (1992).

61. *See* GLENN C. LOURY, ANATOMY OF RACIAL INEQUALITY 30 (2002).

62. For a discussion of the stereotype-threat literature, see Kang & Banaji, *supra* note 9, at 1086-90.

63. *See* LOURY, *supra* note 61, at 38-39; *see also* Daria Roithmayr, *Barriers to Entry: A Market Lock-in Model of Discrimination*, 86 VA. L. REV. 727 (2000) (applying positive feedback loop analysis to White dominance in the legal profession); Daria Roithmayr, *Locked In Segregation*, 12 VA. J. SOC. POL'Y & L. 197 (2004) (following similar analysis to examine residential segregation as a locked-in monopoly).

assumption.

In the net context, the analogous syllogism goes something like this. Broadband providers are rational. Discrimination is irrational, in that it does not further their self-interest. Therefore, broadband providers will simply not discriminate, and ham-fisted regulation is unnecessary. As the talking point goes, net neutrality is a solution in search of a problem. In still more colloquial terms, don't worry, be happy. Among others, Jim Speta[64] and Phil Weiser[65] have invoked such arguments in suggesting that broadband providers, even if monopolists, will not discriminate in adjacent markets for content or application services.

There are many questions here. First, is discrimination actually irrational in the sense that it would not be in the firm's self-interest? For both the "single-monopoly profit" rule and the principle of "internalizing complementary efficiencies" ("ICE principle") there are well-known and less well-known exceptions.[66] Second, even if non-discrimination would be in the firm's self-interest, can we assume that firms will act rationally in the vertical integration context? If the question is articulated as whether managers of broadband firms can write out the economic proofs of the ICE principle, the answer is no.[67] More seriously, we have numerous examples in which firms with market power do not seem to behave rationally. Phil Weiser and Joseph Ferrell call them "incompetent incumbents."[68]

But again, this may be a strawperson. Even if a single firm behaves irrationally, surely the market in its grand totality acts "as if" it were rational. But this survival of the fittest assumption applies best to highly competitive markets with low barriers to entry. In broadband, we have highly centralized markets — typically duopolies with high entry barriers.[69] And where we have such concentration, there is little reason

64. *See* James B. Speta*, Handicapping the Race for the Last Mile?: A Critique of Open Access Rules for Broadband Platforms*, 17 YALE J. ON REG. 39, 76 (2000) ("It is against the platform owner's interest to attempt to monopolize content — even if the platform owner is a monopolist in transmission service.").

65. *See* Phil Weiser, *Paradigm Changes in Telecommunications Regulation*, 71 U. COLO. L. REV. 819, 834 (2000).

66. For well-known exceptions, see van Schewick, *supra* note 23, at 17-25. For more novel exceptions, see *id.* at 9-16.

67. For definitions, see *id*. at 8.

68. Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 114-17 (2003).

69. *See, e.g.*, S. DERRICK TUCKER, FREE PRESS, CONSUMERS UNION & CONSUMER FED'N OF AM., BROADBAND REALITY CHECK II 19-21 (2006) (reporting that cable by itself accounts for 58 percent of residential and small business lines, that cable and DSL together constitute 98 percent of the broadband market, and that 40 percent of U.S. ZIP codes have one or fewer broadband providers), *available at* http://www.freepress.net/docs/bbrc2-final.pdf.

to think that market competition will enforce rationality.[70]

This rationality discussion raises two other points. First, we ought to be cautious about the value of explicit self-reports. Having entered the post-civil rights era, social scientists have struggled with the "willing and able" problem in trying to gauge current stereotypes and attitudes toward various racial groups. Explicit surveys are no longer very useful because, first, people are no longer willing to tell social scientists what they really think about sensitive matters. Respondents instead engage in impression management to sound politically correct. Even when individuals are sincere, research in implicit social cognition has demonstrated that we lack introspective access to various mental constructs, even as those constructs influence our evaluations and behavior.

Interestingly, a similar "willing and able" problem exists in the net discrimination context. All sides of the debate agree that we would benefit enormously from real data on whether broadband providers do in fact have an incentive to discriminate, and whether they will do so.[71] The FCC just launched a Notice of Inquiry to help fill this void.[72] But getting good data is difficult for some of the same reasons outlined above. First, it seems naïve to take at face-value what firms promise publicly because they are managing impressions to stave off potential regulation.[73] Second, even if firm representatives sincerely believe that the firm's private interest aligns fully with the public's interest in maximum innovation and social welfare,[74] they may lack introspective

70. To be sure, many are now relying on intermodal competition, as telephone companies go after cable companies with wireless and powerline carriage in the works. However, such competition is more incipient than extensive. *See* Herman, *supra* note 31, at 137.

71. Many broadband service providers have contractual terms that afford them great license over the content transported through their pipes. *See, e.g.*, *id.* at 126 (citing examples from Cox, AT&T, and the Canadian firm Telus).

72. *See* Broadband Industry Practices, *Notice of Inquiry*, 22 FCC Rcd. 7894, ¶¶ 8-11 (2007).

73. Commentators have, however, accumulated some revealing exclamations. *See, e.g.*, Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 934 (2001) (reporting that AT&T's Jack Osterman said of early plans for the Internet, "[f]irst . . . it can't possibly work, and if it did, damned if we are going to allow the creation of a competitor to ourselves."); *At SBC, It's All About "Scale and Scope"*, BUS. WK., Nov. 7, 2005, http://www.businessweek.com/magazine/content/05_45/b3958092.htm (quoting AT&T Chairman Ed Whitacre as saying "[n]ow what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes? The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!").

74. For skepticism on this point, see Baker, *supra* note 39, at 751. He points out the difference between enterprise-based and welfare-based economics. For example, cost savings that are "efficient" for the enterprise/firm may not be "efficient" for all of society.

access to the various implicit cognitive processes in individual managers' heads and implicit organizational processes in firm practices that produce self-serving forms of discrimination.[75]

The other point concerns the normative addendum to the rough syllogism. That addendum suggests that any "discrimination" that is in fact rational should be normatively tolerated. Put another way, instrumental rationality should necessarily purchase normative acceptability. But there are many objections to this argument, and current antidiscrimination law rejects it.[76] In the net context, this rationality justification seems especially weak since the private interest may only poorly align with the public interest. Since broadband access is an infrastructural good and because the broadband provider cannot capture and monetize the positive externalities, its rational decisions to pursue its private interest may substantially harm public welfare.

Here is one final concern about what rationality is supposed to buy. In the race context, suppose someone defends her action as responding on the basis of accurate base rates that distinguish between racial groups. A thoughtful person might ask *why* do the base rates differ? Nature? Nurture? Some inextricable mix of both? What if part of the reason for the difference is the normatively problematic past? If we ignore such a history, then our instrumentally rational actions today might fuel yet another cycle in a positive feedback loop, which locks in past injustices.

Surprisingly, there are parallels for net discrimination. When a broadband provider makes rational decisions to maximize its private welfare, we must understand that such a calculation depends on the firm's current conditions, which were produced by a specific, historically contingent path. And with broadband providers, that path often included the privilege of legal monopoly, usage of public property at little or no cost, and benefit from network economics that cement first-mover advantage. For example, telephone companies were historically monopoly franchises, granted the right to use public right-of-ways for private profit. If we decide to correct the past, that is, move away from legal monopoly (*cf.* the legal monopoly of Whiteness and segregation)

---

75. Richard Nelson and Sidney Winter point out that firms operate on process schemas, a sort of automatic pilot, with limited ability to process an overwhelming flow of information. RICHARD R. NELSON & SIDNEY G. WINTER, AN EVOLUTIONARY THEORY OF ECONOMIC CHANGE 14 (1982); *see also* Lemley & Lessig, *supra* note 73, at 937 (discussing how firms develop core competencies, protect legacy businesses); *id.* at 950 (discussing possibility of corporate endowment effect); *id.* at 944-45 (pointing out that explicit intent is not necessary for monopolist pipe owners to skew innovation in their favor and towards familiar technologies and existing expertise).

76. City of Los Angeles, Dep't of Water & Power v. Manhart, 435 U.S. 702, 716 (1978) (actuarially justified sex-differentiated employee contributions to employer pension plan are disparate treatment). *See generally* Samuel R. Bagenstos, *"Rational Discrimination," Accommodation, and the Politics of (Disability) Civil Rights*, 89 VA. L. REV. 825 (2003).

towards a level playing field (*cf.* desegregation and the civil rights movement), we cannot expect to do so simply by formally ending legal monopoly, then allowing the incumbent to do whatever is in its self interest — especially when network effects inure to the incumbent's benefits.[77] That would cement past privilege into present advantage. We certainly understood the basic economics — if not the actual implementation — when we tried to introduce competition into the local exchange.[78]

In sum, the race discrimination debate teaches us to be more skeptical about optimistic and self-serving claims that rationality will burn away net discrimination, and leave behind only normatively acceptable byproducts. First, we may not act as rationally as we hope and trust we do. Second, even when we are instrumentally rational in pursuing our private interests, that may not further the public's interest, which might include both deontological (e.g., corrective justice) and welfarist ambitions (an infrastructure for innovation and communicative participation).

CONCLUSION

This essay is another one of my attempts to cross-pollinate the race and communications literature.[79] A comparison and contrast between race discrimination and net discrimination teaches us, first, to particularize the discrimination at issue and be wary of normative carve-outs in defining discrimination. Second, we must recognize and respect the clash between welfarist and deontological concerns. Third, we should beware of assurances that private rationality guarantees public interest.

These insights do not translate into specific policy recommendations; they were never meant to. For readers yearning for something more concrete, I only offer some doctrinal gestures. As explained above, we must always particularize the discrimination at issue — which entity X is being treated differently on the basis of which attribute Y? In this specification, it may or may not be useful to think in terms of "suspect classifications" that borrow from equal protection doctrine or bona fide occupational qualifications ("BFOQs") that borrow

77. Lee, *supra* note 7, at 1266.

78. The Telecommunications Act of 1996 insisted on no monopoly franchises, see 47 U.S.C. § 253(a) (2000), and demanded interconnection to counter network effects, see § 251(a)(1) (all carriers), and § 251(c)(2) (special requirements for incumbent local exchange carriers).

79. *See, e.g.*, Kang, *Cyber-race*, *supra* note 8 (analyzing how the social construction of race may unfold in the technological construction of cyberspace); Kang, *Trojan Horses*, *supra* note 9 (analyzing mass media policy in light of implicit social cognition).

from Title VII. But the more relevant analogy is to First Amendment law, with its greater skepticism of content-based regulations as compared to constraints on mere time, place, or manner. This doctrinal analogy would underscore the importance of the first of the FCC's "Four Freedoms" on net neutrality: the right to access all lawful content.[80] It would also support the nondiscrimination provision attached to the recent AT&T and Bell South merger,[81] which the Net Neutrality Notice of Inquiry floats as a potential general principle.[82]

I conclude by asking an odd question: what is the value of common carriage?[83] Imagine that after converting to all IP networks, telephone companies simply declared that they were no longer common carriers. Instead, they were providing "information services," and in fact, similar to cable operators, were engaged in constitutionally protected speech.[84] What if the telephone companies then ensured better quality connections to their preferred customer partners (say Expedia's travel agents over Priceline's) who paid them a kick-back? Even more extreme, what if a telephone company, controlled by an activist media mogul, implemented software algorithms to disconnect calls that seem to facilitate terrorist agendas or titillate with prurient language?

This is not so crazy. AT&T as broadband service provider intends to scan for what it thinks to be illegally copied content;[85] Google as video hosting service is taking down sniper clips (which by themselves are offensive but not illegal);[86] and in 1992, Congress granted to cable operators the right to censor prurient content that would appear on leased

---

80. *See* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Policy Statement*, 20 FCC Rcd. 14,986, 14,988 (2005). The four principles set out in this policy statement embody the "Four Freedoms" identified by former Chair Michael Powell: freedom (i) to access lawful content, (ii) to use applications and services of their choice (subject to law enforcement), (iii) to attach legal devices to the network that do no harm, and (iv) to enjoy competition among providers. *See* Michael K. Powell, FCC Comm'r, Address at the Silicon Flatirons Telecommunications Program Conference: Reflections on Communications Policy (Nov. 13, 2000).

81. *See* AT&T Inc. & BellSouth Corp. Application for Transfer of Control, *Memorandum Opinion & Order*, 22 FCC Rcd. 5662 app. F at 5814 (2007) ("AT&T/BellSouth also commits that it will maintain a neutral network and neutral routing in its wireline broadband Internet access service. This commitment shall be satisfied by AT&T/BellSouth's agreement not to provide or to sell to Internet content, application, or service providers, including those affiliated with AT&T/BellSouth, any service that privileges, degrades or prioritizes any packet transmitted over AT&T/BellSouth's wireline broadband Internet access service based on its source, ownership or destination."). The focus on "source, ownership or destination" is in effect a proxy for content-based discrimination.

82. *See* Broadband Industry Practices, *supra* note 72, at ¶ 10.

83. In a prescient article, Eli Noam predicted the end of common carriage. *See* Eli M. Noam, *Will Universal Service and Common Carriage Survive the Telecommunications Act of 1996?*, 97 COLUM. L. REV. 955 (1997).

84. *See* Leathers v. Medlock, 499 U.S. 439, 444 (1991).

85. *See* Granelli, *supra* note 15.

86. *See* Wyatt, *supra* note 16.

access and PEG (Public, Educational, and Government) channels.[87] In fact, in his concurrence in *Sable Communications of California v. FCC*,[88] Justice Scalia suggested that even telephone companies — notwithstanding their public utility status — could drop dial-a-porn callers if they so choose.[89]

I think most telephone users would think all of this to be odd and disturbing. Sure, television stations and networks control what can be seen on TV; cable operators control what can be seen on cable; websites control what content can be downloaded from their servers. But the telephone? Even the telephone company gets to control who says what to whom? What's more, these firms could benefit all the while from 47 U.S.C. § 230, which shields "interactive computer service" providers with nearly bulletproof immunity.[90] In other words, they would receive the central benefits of common carriage, but bear none of the costs.

My question is hypothetical because regulators would probably never allow this convenient opting out of common carriage. This is apparent from the FCC's regulatory approach toward VoIP, which follows the basic principle that if it works like a traditional telephone from the end-user's perspective, it will be regulated like a traditional telephone.[91] But why couldn't the same arguments against net neutrality regulation be deployed against common carriage regulation for telephones? If we must keep "hands off the Internet," why not also keep our grubby regulatory "hands off the telephone"?

With only modest creativity, telco executives could assert that the next generation of fancy telephone networks (4G) will only be built if they can shed the legacy vestiges of common carriage. Not just fringe regulations, mind you, but the core obligations against unreasonable discriminations and preferences.[92] When that plea comes, my guess is

---

87. *See* Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727 (1996).

88. 492 U.S. 115, 132-33 (1989) (Scalia, J., concurring).

89. *See id.* at 133 ("I note that while we hold the Constitution prevents Congress from banning indecent speech in this fashion, we do not hold that the Constitution requires public utilities to carry it.") (Scalia, J., concurring).

90. Section 230(e)(3) states that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." 47 U.S.C. § 230(e)(3). This immunity does not apply, however, to intellectual property claims, criminal prosecutions, and claims under the Electronic Communications Privacy Act. *See generally* KANG, *supra* note 13, at 392-94.

91. *See, e.g.*, Universal Service Contribution Methodology, *Report & Order & Notice of Proposed Rulemaking*, 21 FCC Rcd. 7518, ¶¶ 3, 48-49 (2006) (requiring interconnected VoIP providers to start contributing to the universal service fund, without definitively deciding whether they are an information service or telecommunications service); Federal-State Joint Board on Universal Service, *Report*, 13 FCC Rcd. 11,501, ¶¶ 87-90 (1998) (distinguishing computer-to-computer IP telephony from phone-to-phone IP telephony).

92. *See* 47 U.S.C. § 202, which states:

> Discriminations and preferences.

that there would be a pause. And again, rightly so.

(a) Charges, services, etc.
It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage.

NETWORK NEUTRALITY: REGULATING WITH MORE QUESTIONS THAN ANSWERS

HOWARD A. SHELANSKI*

INTRODUCTION

"Network neutrality," while subject to varying definitions, can be summed up as the principle that "all like Internet content must be treated alike and move at the same speed over the network. The owners of the Internet's wires cannot discriminate."[1] The policy implication is that network operators should not be allowed to "create different tiers of online service" by selling different levels of access at different prices to different providers of on-line content and services.[2]

Proposals for network neutrality regulation have sparked particularly intense debate. Advocates and opponents of regulation have each predicted dire consequences from, respectively, leaving networks free to vary terms of access they offer to upstream providers of content and services[3] or restricting them from doing so. As the debate has continued between those who argue that network neutrality regulation is necessary to preserve applications innovation and those who argue that such regulation would harm the growth and development of underlying network infrastructure, Congress has been awash with legislative proposals from both perspectives.[4]

---

* Professor of Law, University of California at Berkeley. This essay is based on the author's presentation at the Silicon Flatirons Digital Broadband Migration Conference, February 19-20, 2006, University of Colorado, Boulder. The author is grateful to Joe Farrell, Larry Lessig, Jim Speta, Barbara van Schewick, and Phil Weiser for helpful comments and discussions.

1. Lawrence Lessig & Robert W. McChesney, *No Tolls on the Internet*, WASH. POST, June 8, 2006, at A23, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html.

2. *Id.*

3. I will refer to providers of Internet content and services generically as "applications providers" for the rest of this essay.

4. *See* ROBERT D. ATKINSON & PHILIP J. WEISER, INFO. TECH. & INNOVATION FOUND., A "THIRD WAY" ON NETWORK NEUTRALITY 2 n.3 (2006), http://www.itif.org/files/netneutrality.pdf.

Why such attention to network neutrality? The reason may lie in the fact that, although vertical issues have long been central to telephone regulation,[5] the stakes for consumers have changed with the Internet. Only a few years ago, the principal value of the telephone network to consumers was person-to-person voice communication and the principal value of cable networks was video programming. Complementary, vertical services like voice mail or information services were comparably modest in importance. Now, those same networks deliver a vast universe of content and services through the Internet. Some such services, for example Internet telephony ("VoIP") or video services ("IP-TV"), may compete directly with the core services of the underlying networks. But most services are complements, not competitors, to the networks over which consumers reach the Internet, and there is enormous value in those complementary applications. Telephone and cable networks have gone from wagging the tail to wagging the dog with respect to vertical services and their importance to consumers. While the increasing value of the applications market gives rise to concern over vertical discrimination, it simultaneously raises the potential benefits of vertical relationships between networks and applications providers.[6] Particularly for new and commercially risky applications, vertical relationships can, at least theoretically, reduce transaction costs and bring new products and services to market faster. Not surprisingly, therefore, network neutrality regulation has both its advocates and opponents who speak in adamant terms about the consequences of either allowing network owners to discriminate among applications providers or barring them from doing so.

Proponents of regulation confidently argue that discriminatory access terms will chill innovation at the edge of the network, reducing the flow of new services and applications for consumers.[7] Opponents argue with equal force that a ban on discrimination will dampen innovation and investment in the core of the network, reducing capacity and shifting costs to consumers.[8] Applications providers argue that

---

5. *See* STUART MINOR BENJAMIN ET AL., TELECOMMUNICATIONS LAW AND POLICY chs. 13-14 (2d ed. 2006).

6. *See, e.g.*, Oliver E. Williamson, *Assessing Vertical Market Restrictions: Antitrust Ramifications of the Transaction Cost Approach*, 127 U. PA. L. REV. 953 (1979); Oliver E. Williamson, *The Vertical Integration of Production: Market Failure Considerations*, AM. ECON. REV., May 1971, at 112.

7. *See, e.g.*, *Net Neutrality: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 54-59 (2006) (prepared statement of Lawrence Lessig), *available at* http://www.lessig.org/blog/archives/lessig_testimony_2.pdf.

8. *See, e.g.*, Christopher Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 27-28 (2005); Bruce M. Owen, *The Network Neutrality Debate: 25 Years after AT&T v. United States and 120 Years After the Act to Regulate Commerce*, PERSP. FROM FSF SCHOLARS (Free State Found., Potomac, Md.), Feb. 20, 2007,

discriminatory pricing will unfairly target deep-pocket providers or firms that compete with the platform's own vertical services.[9] Platform providers argue that they have no incentive to make the Internet less attractive to their subscribers and that successful applications providers are free riding on their networks.[10] Each side claims to champion competition and innovation while portraying the other as being something between an opportunist and a gangster.[11] Upon closer inspection, however, each side's arguments beg important questions to which answers are both empirically and theoretically elusive. Those open questions, in turn, weaken the basis for either the outright ban on discrimination sought by network neutrality advocates or the pure laissez-faire sought by its opponents.

This essay will briefly examine several unanswered questions central to the network neutrality debate and discuss their implications for broadband policy. Part I of this article will examine the main claims made by each side of the network neutrality debate and discuss the unanswered questions upon which the merits of those arguments depend. Part II will analyze the policy implications of those unanswered questions, examine the balance of risks at issue in network neutrality regulation, and discuss how policy should account for those risks in the presence of incomplete information.

I. STRONG ASSUMPTIONS ABOUT REGULATING (OR NOT)

Proponents of network neutrality regulation contend that discriminatory network access terms will selectively impede applications providers' access to consumers and thereby chill innovation at the edge of the network (meaning innovation by those who use the network as a medium for providing their content and services to consumers), reducing the flow of new services and applications to the market. They contend that discrimination would force potential innovators either to buy a costly level of access or risk providing a second-class service with reduced priority to the conduits that reach consumers and, in turn, reduced chances for commercial success. Either choice imposes costs that will cause applications developers on the margin to engage in less innovation.

---

http://www.freestatefoundation.org/images/The_Net_Neutrality_Debate-Bruce_Owen.pdf.

9. *See* Letter from Jeff Bezos, Founder & CEO, Amazon.com, et al., to Joe Barton, Chairman of U.S. H. Comm. on Energy and Commerce et al. (Apr. 5, 2006), *available at* http://markey.house.gov/docs/telecomm/CEO%20Letter.pdf.

10. Online Extra, *At SBC, It's All About "Scale and Scope"*, BUS. WK., Nov. 7, 2005 (quoting SBC CEO Edward Whitacre on free riding by applications providers), *available at* http://www.businessweek.com/@@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm.

11. Tim Wu, *Why You Should Care About Network Neutrality: The Future of the Internet Depends on It!*, SLATE, May 1, 2006, http://www.slate.com/id/2140850/.

Advocates thus argue that a level, or neutral, playing field for all applications providers is necessary to preserve the ability of intelligence at the "edge" of the network to drive innovation and increase the welfare of consumers.

Arguments against network neutrality often rest on the similar, but diametrically opposed, proposition that investment and innovation will suffer unless network owners can recover costs imposed by high-volume applications. The innovation at issue here is not at the edge of the network but at its "core." At issue is the need for capacity, reliability, and security for traffic moving across the network. Some network owners argue that the content and service providers whose applications generate the traffic should pay for the capacity to carry it to end users. From this perspective, applications providers impose costs on networks and should bear them accordingly, not shift them to network owners or subscribers. Network operators argue that they have no incentive or ability to exclude or reduce the appeal to consumers of any upstream applications, because those applications are what attract subscribers to their networks. They also note that some applications innovators on the edge of the network might be deterred not by discrimination, but by neutrality, because they will be unable to secure priority access from the network operator for services that need to run with a particular assured quality.

Each set of arguments above raises difficult empirical and theoretical questions, and each depends to some extent on the competitive dynamics of the network access market. The more networks there are in competition with each other for subscribers, the less easily can any individual network engage in inefficient discrimination against particular applications or applications providers. Consumers will choose networks that get them the content and services they want fast and reliably. Which side of the debate one credits will therefore depend, at least in part, on one's view of how competitive the market is and will be.

A. Discriminatory Access and Applications Innovation

Even assuming all applications innovation to be welfare improving, what basis is there for determining how much, if any, innovation deterrence would result from discrimination by platforms in terms of access offered to applications providers? Two proponents of network neutrality regulation offer the following empirical motivation for their claim that non-neutrality would deter innovation:

> More than 60 percent of Web content is created by regular people, not corporations. . . . Most of the great innovators in the history of the Internet started out in their garages with great ideas and little capital. This is no accident. Network neutrality protections minimized

> control by the network owners, maximized competition and invited outsiders in to innovate. Net neutrality guaranteed a free and competitive market for Internet content. The benefits are extraordinary and undeniable.[12]

Taking the above argument to be true, the fact that innovators thrived under a neutral regime does not itself tell us how many of those innovators would have been deterred had network operators offered a tiered set of offerings in which quality rose with price. The empirical observation that has motivated some to advocate network neutrality thus does not necessarily supply empirical support for the innovation deterrence argument on which that advocacy largely rests.

Nor is the logical or theoretical connection between neutrality and applications innovation so clear that the network neutrality advocates' innovation-deterrence argument should be accepted as a matter of reason. First, at least some applications providers may be deterred by the absence of a high-priority tier of access. Some services, for example video services, may need reduced latency to work well, and absence of an assured level of priority raises the risk that such services will fail to live up to their billing, hence deterring their introduction.

Second, there is no reason to assume that most services will in fact be harmed if they are transmitted with the base (*i.e.* lower) level of priority. Comparatively low-bandwidth applications may work perfectly well at lower tiers of access and their innovation might not depend on neutrality. Moreover, even if there is some quality effect, consumers have shown a willingness to tolerate slower interactions on the Internet in return for lower subscription prices. Success of an application, therefore, may not depend on purchasing a costlier tier of access from network operators, especially where there is some way to compensate consumers for any delays in service.

Third, even if neutrality was a causal factor in the explosion of innovation from the edge of the network in the first decade of the commercial Internet, that same environment need not be optimal for the next decade of a more mature Internet. It bears noting that in key areas of commerce, content, and applications, the on-line world is populated by a handful of major players. The brand-name recognition, installed base of customers, and network externalities accumulated by established on-line players could present much greater obstacles in some lines of internet applications than would discriminatory access terms. Indeed, it is precisely the established players who fear non-neutrality because they may be natural, deep-pocket targets for aggressive access negotiation by network operators. Neutrality regulations would protect them from such

12. Lessig & McChesney, *supra* note 1.

pressure.

Neutrality may, however, also benefit established players in another way, this one less sympathetic or potentially beneficial for innovation: access quality may be an important way for new competition in some services to differentiate themselves from incumbents. Established applications providers have little interest in defending against entrants on new competitive dimensions. The "neutral" status quo may therefore be of competitive advantage to applications incumbents while denying a competitive tool to new innovators from the edge.

Finally, platform competition was less developed during the early years of the commercial Internet. Few Americans (19 percent) even had Internet access at all from their homes in 1996, while today most have computers and a choice of broadband access providers.[13] Even if neutrality was necessary to speed applications innovation under the early years of limited broadband availability and no choice of broadband providers, it is unclear that it would be in today's more competitive environment.

The arguments made above do not refute the possibility that non-neutrality will deter applications innovation. They do, however, show that there is little reason to presume such an effect for policy purposes and good reason to question whether non-neutrality will cause the severe harms that some network neutrality proponents suggest. The case for such harmful effects diminishes with increased network competition. Under duopoly, the case is ambiguous. As wireless platforms enter the market to compete against the cable and telephone networks, the ability of any network to discriminate inefficiently by artificially slowing selected traffic to sell priority declines because its rivals will have incentives to offer consumers greater assurance of fast content delivery.

B. Networks and Incentives to Discriminate

Consider next the incentives of network owners to engage in discrimination that harms innovation or consumer welfare. Opponents of network neutrality regulation have argued that network owners would have no incentive to discriminate against applications providers in a way that made network subscription less attractive to consumers. Underlying this claim is the idea that "a monopolist—which, by definition, would have the ability to impede competition in adjacent markets—generally will have no incentive to do so" because it cannot enlarge its profits by doing so.[14] Any reduction in value (or increase in price) of the upstream

13. Press Release, FCC, Federal Communications Commission Releases Study on Telephone Trends (June 21, 2005), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/trend605.pdf.

14. James B. Speta, *The Vertical Dimension of Cable Open Access*, 71 U. COLO. L. REV.

application will be met by a corresponding reduction in demand (or decrease in profits) for platform subscriptions, a phenomenon that Joseph Farrell and Philip Weiser have labeled "*internalizing complementary efficiencies*" or "ICE."[15]

Farrell and Weiser demonstrate, however, that while ICE often holds, under many conditions it does not. As Farrell explains, platform owners can often raise their profits by price discrimination, and even if one assumes the price discrimination itself to be efficient (which is not always the case), platform owners may discriminate against providers of complementary services in order to facilitate price discrimination.[16] Farrell illustrates his point through the simple example of a copy machine manufacturer that wishes to price discriminate by selling the copier at a low price and metering use through sale of repair services.[17] In order for repair services to be a metering mechanism for price discrimination, the copier manufacturer must receive revenues for all repairs done to its copiers. One way the manufacturer can do this is to withhold spare parts from independent repair firms and to do all the repairs itself, eliminating competition and reducing efficiency in the complementary repair market. Thus, the non-neutrality of the mechanism used to accomplish price discrimination can involve what Farrell has termed "collateral-damage inefficiency."[18] The important point is that whether or not the underlying price discrimination is itself efficient, that discrimination can be profitable for the manufacturer despite any collateral-damage inefficiency it might cause.

In theory, the manufacturer could avoid this collateral damage through other means of metering. For example, instead of making repair services the metric, the manufacturer could make spare parts the metric and then meter usage of the copier through sales of spare parts to all providers of repair services. Copier owners would retain their choice of service providers and the most efficient service providers would remain able to compete for repair business. To the extent that more efficient metering mechanisms are harder to administer than preemption of competition in the complementary market, however, firms may opt for the latter despite the inefficiency.[19]

975, 997 (2000).

15. Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 89 (2003).

16. Joseph Farrell, *Open Access Arguments: Why Confidence is Misplaced*, *in* NET NEUTRALITY OR NET NEUTERING: SHOULD BROADBAND INTERNET SERVICES BE REGULATED? 195, 199 (Thomas M. Lenard & Randolph J. May eds., 2006).

17. Farrell does not use this example in his 2006 paper but did so in discussions with the author.

18. Farrell, *supra* note 16, at 199.

19. *See, e.g.*, Eastman Kodak Co. v. Image Technical Servs., Inc., 504 U.S. 451, 478

In the context of network neutrality, the pursuit of price discrimination could lead to harmful departures from neutrality toward upstream applications. While Farrell and Weiser show that platform owners may have incentives to discriminate inefficiently where the application competes with a core service of the platform[20] (*e.g.* VoIP for telephone networks or video-on-demand for cable networks), harm may still result even when the upstream application is not one that rivals the platform's main line of business. For example, one mechanism a cable network owner could use to price discriminate is to bundle Internet access with some application, say IP telephony. The network could offer consumers two choices: Internet access for $30 per month, or Internet access for $25 per month if the consumer also subscribes to the network operator for IP telephone service. To make this bundle profitable, the network operator not bound by network neutrality rules might discriminate in the terms of access it provides to rival IP telephone providers to put them at a competitive disadvantage. So long as the increased attractiveness of Internet subscriptions due to the $5 discount outweighs the decrease in attractiveness due to the reduced choice of IP telephone services, the network operator may find the collateral damage to the upstream applications market nonetheless to be profitable. The same scenario could hold for other means of price discrimination, say a phone company's metering of subscribers' Internet usage through video downloads or some other application susceptible to incremental charges.

This is not to say that there are no possible welfare benefits from the price discrimination described above. By using discrimination — whether through bundling, metering, or some other mechanism — to extract high surplus from one set of users, a network operator may enable another set of users to have access where they would not under a single-price regime. This is particularly so in the case for high-fixed-cost services like Internet access, where price discrimination might allow a network to offer some subscribers access at prices closer to marginal cost because it is recovering its fixed costs from other, higher-paying, customers. It is this very ambiguity in the welfare effects of price discrimination and in the incentives to discriminate inefficiently that is important. The welfare ambiguity means that any rule patently barring discrimination could have unintended, negative consequences because the conduct sought to be barred — price discrimination — is neither always bad nor always good.

(1992) (alleging vertical foreclosure by Kodak as a means to leverage profits).

20. *See* Farrell & Weiser, *supra* note 15, at 108.

C. Capacity, Efficient Priority Choices, and Network Investment

A third set of questions in the network neutrality debate revolves around network capacity. If capacity is not scarce, then there is no need for networks to prioritize one provider's traffic over another and no need for investment in new capacity. Capacity thus implicates two important issues for the network neutrality debate. The first is whether upstream price discrimination is necessary to establish priority; the second is whether upstream price discrimination is necessary to recover the costs of investing in new capacity and network technology. The threshold question underlying both of these questions is whether capacity is scarce such that congestion will at least sometimes occur and require networks to prioritize one packet of information over another. If not, then it is hard to see what good could emerge from departures from neutrality, as such departures could be aimed neither at efficiently prioritizing traffic, nor at efficiently recovering network investment.

There may be little agreement over the exact extent of current or future capacity constraints on broadband networks, but neither is there evidence that capacity is so plentiful that congestion, and hence the issue of priority, never arises. Indeed, one report argues that new capacity investment is necessary and that the market does not currently provide adequate incentives for network owners to make such investments.[21] The head of television technology for one of the strongest advocates of network neutrality, Google, in a widely reported statement also emphasized the need for core investment when he said "[t]he Web infrastructure and even Google's (infrastructure) doesn't scale. It's not going to offer the quality of service that consumers expect."[22] Given that capacity constraints cannot be assumed away in the network neutrality debate,[23] the question becomes whether they can supply any justification for differentiating among applications providers in the terms of network access.

One rationale for allowing price discrimination is that it provides a basis for deciding which packet should take priority over another. This is exactly what raises concern among network neutrality advocates; new

---

21. DELOITTE TOUCHE TOHMATSU, TELECOMMUNICATIONS PREDICTIONS: TMT TRENDS 2007 8 (2007), *available at* http://www.deloitte.com/dtt/cda/doc/content/us_tmt_%202007_Telecom_Predictions_011606.pdf.

22. *Google and Cable Firms Warn of Risks From Web TV*, USA TODAY, Feb. 7, 2007 (quoting Vincent Dureau), *available at* http://www.usatoday.com/tech/news/2007-02-07-google-web-tv_x.htm.

23. Indeed, such an assumption implies either that the marginal value of investment in the core platform infrastructure is zero or that it is always lower than the marginal value of applications innovation. As discussed below, there are many unknowns about the relevant incentives to innovate and about the marginal benefits to consumers of different innovations; but the evidence suggests that the core cannot simply be ignored in favor of the edge.

applications providers will have to either pay or sit in line.[24] As discussed above, charging for priority may or may not have a significant negative impact on applications innovation. But if there really is a need to prioritize, it is important to examine the alternatives before ruling out price mechanisms. The most neutral alternative of random selection would serve consumers poorly. A spam e-mail is likely to be less valuable to either consumer or provider than a VoIP call or a paid music download. Random selection could lead the spam to be delivered first, however, benefiting no one except the provider of the lower-value service.

A more nuanced alternative is suggested by the definition of network neutrality at the beginning of this article: "all *like* . . . content must be treated alike and move at the same speed."[25] Under a close reading of this definition, it might be fine for the network to prioritize VoIP over e-mail, so long as all VoIP were treated the same and all e-mail were treated the same. While such hierarchy of uses might be better than random prioritization, it still raises potential problems because it puts the network owner in the position of having to decide which uses or categories of content should be prioritized over others, which uses are "like" other uses, and where innovative new uses should be placed in the priority queue. Defining a clear and administrable regulatory standard for "like content" will prove difficult.

Creating a market for priority can alleviate the difficulties with random or "like use" prioritization and reduce the allocative inefficiency that can result from those mechanisms. Network investment could become more efficient because firms with a desire for priority will capture direct private benefits (less delay for their packets) of their payments to the network operator. When the network owner or subscribers must bear the costs, the benefits are more diffuse, creating the potential for underinvestment. Moreover, to the extent price discrimination allows more highly valued information to move faster, it has the potential to increase the efficiency and consumer welfare of Internet activity. On the other hand, to the extent price discrimination is used in a targeted way as an anticompetitive strategy to raise the costs of particular applications providers, it can be harmful. Again, the non-neutral strategy can have either (or both) positive and negative effects.

The next question related to capacity is whether recovery of capacity investment supplies a rationale for price discrimination toward applications providers. Networks receive revenues from subscribers, raising the question of why they would need to charge applications providers for access. There are several reasons why recovering network

24. *See*, *e.g.*, Wu, *supra* note 11, at 3.
25. Lessig & McChesney, *supra* note 1 (emphasis added).

costs from subscribers alone might not be optimal. First, even though networks can and do charge subscribers different monthly fees for different Internet access speeds, that pricing mechanism may leave some subscribers who are willing to pay the cost of higher-speed access nonetheless unwilling to pay its price. Within each tier of access, there will be relatively high-usage subscribers and relatively low-usage subscribers. Because all subscribers to a given tier pay the same price, the latter may pay for more speed and capacity then they use while the former pay for less than they use. The subscription price that the relatively low-usage consumers pay is therefore above the costs they impose on the network. Were the subscription price for these users lower and more reflective of their actual usage, they would attract yet lower-usage customers whose willingness to pay was above cost, but not quite up to the existing monthly charge for the higher tier of access. To the extent payments from applications providers can ameliorate this potential inefficiency of consumer-side charges, charging those applications providers can be beneficial.

Second, even if subscription rates can be structured better to reflect each subscriber's actual usage, there may still be inefficiency in on-line consumption. One reason stems from the costs of trying out new, high-bandwidth content and applications. If consumers are paying the full costs of their usage, they may hesitate to try new services that would increase their costs. Some kind of transfer payment from the applications providers to consumers could overcome this inefficiency, although such compensation mechanisms might involve high transaction costs. If applications providers would be willing to pay more to networks in return for subscribers who have faster connections and are more willing to consume various content and services, then it might be more efficient, as well as more profitable, for networks to reduce subscription prices in conjunction with charging applications providers for different levels of access.

Finally, consumers and applications providers may have asymmetric valuations of their interactions. It may be more valuable for applications providers to have consumers use their services than it is for consumers to receive them. This is particularly true where the applications provider is paid by a third party — perhaps an advertiser or search listing — based on the number of people who visit the site. Any given consumer might find the experience worthless and merely "click through" the site. The applications provider may, however, benefit from that very same click-through and therefore, have an interest in reducing the cost to subscribers of accessing their sites. If the network can only charge the consumer for network access, the joint surplus of consumers and applications providers might be lower than it would be if applications providers could pay to speed interactions with, and perhaps reduce prices to, consumers.

The above three reasons why it might not be efficient to charge only subscribers for use of network infrastructure do not resolve the question of whether price discrimination toward applications providers will improve consumer welfare or efficiency. They do show, however, that this issue is complex and that arguments for upstream price discrimination cannot be ignored just because networks already charge subscribers. Internet platforms may well have the attributes of two-sided markets, in which charging end-users and applications providers can be more efficient than placing the charges on one side alone.[26] Whether or not they do, and whether or not the gains from two-sided pricing offset possible costs, are beyond the scope of this paper and are important topics for further research. For current purposes, however, the important point is that the question of the comparative costs and benefits of one-sided versus two-sided pricing is an open one that should not be assumed away on either side of the network neutrality debate.

II. COMPARATIVE RISKS OF ALTERNATIVE FORMS OF NON-NEUTRALITY

The previous section demonstrates that the effects of network non-neutrality toward applications providers are ambiguous, with some possibility that neutrality could deter applications innovation but some possibility too that it could benefit, to varying degrees, network investment, applications competition, and allocative efficiency. Conversely, mandatory neutrality could benefit applications innovation and prevent collateral inefficiencies due to anticompetitive vertical discrimination, but could also reduce the efficiency of investment and the volume and nature of on-line transactions. In neither case, however, are the benefits either sufficiently sure or substantial to justify a policy that pursues one set of objectives (*e.g.* applications innovation) to the exclusion of others (*e.g.* network investment). There are too many open questions about the impact of either laissez-faire or a strict neutrality rule to make a persuasive case for either solution. Either choice is uncertain to achieve its intended objectives and likely to involve tradeoffs and to entail a balance of risks with respect to other beneficial objectives.

This section argues that the policy choice need not be as stark as that between complete neutrality and unrestrained laissez-faire. Discrimination varies in its motivations and methods, and different kinds of network discrimination differ in the balance of risks they entail for networks, applications providers, and consumers. Regulation that restricts some forms of discrimination but not others might protect against the worst harms of non-neutrality without eliminating some of

26. *See* Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report*, 37 RAND J. ECON. 645 (2006), *available at* http://idei.fr/doc/wp/2005/2sided_markets.pdf.

the investment and efficiency benefits that differentiated access terms for applications providers might allow.

A. Reasons for a Network to Discriminate

Several things might motivate a firm to discriminate in the terms it offers to customers or providers of complements. At the broadest level, a firm might discriminate because it must due to scarcity. In the network context, a firm might be driven to sell priority because congestion requires packets to be dropped at times. In such a case, discrimination could take the weak form of granting priority to some packets only when the capacity constraint binds. An analogy might be a traffic lane that is reserved for eligible vehicles only at rush hour, but is open to general use at other times. This kind of discrimination is what Edward Felten calls "minimal discrimination."[27]

Alternatively, a firm might sell priority because it can manipulate traffic in either beneficial or harmful ways. The analogy here is to a special traffic lane that is reserved all the time, even at times when there would be no congestion were that lane open to use by all. The result could be to raise the probability of delay on the non-reserved lanes, thus attracting customers who won't risk moving slowly and want an assurance of moving quickly at all times. This kind of discrimination is what Felten calls "non-minimal" or "delay" discrimination.[28] Such discretionary prioritization is not necessarily inefficient, depending on the relative costs of delay to those users that incur the delay and those that pay to avoid it. It does, however, raise the prospect of inefficiency and anticompetitive manipulation. Even at this general level there are different risks of harm to competition and innovation. Discrimination driven by necessity that occurs only when capacity constraints bind runs less of a risk of harm than discrimination that is driven by market power and the ability to manipulate traffic.

Discrimination could be further motivated by a number of more specific forces that work in tandem with those motivations discussed above. For example, a network could discriminate against an applications provider as part of an anticompetitive strategy to harm an application or provider that the network does not like, perhaps to shift market share of a complement to the network operator. Alternatively, the network could discriminate because it realizes that some providers are willing to pay more if pushed to do so, thus shifting surplus from the applications provider to the network operator.[29] Or, the network could

27. Edward Felten, *Nuts and Bolts of Network Neutrality*, 6 J. ON TELECOMM. & HIGH TECH. L. (forthcoming 2008).

28. *Id.*

29. Such arguments are sometimes framed as a claim that some applications providers are

price discriminate to recover operating expenses or investment from those applications providers who cause the network to incur higher costs, thus shifting costs from the network operator to the applications provider. Again, each of these motivations entails different risks to competition and innovation, with raising rivals' costs being the most harmful motivation and cost-recovery being the most consonant with competition and innovation.

B. Methods of Network Discrimination

Next, consider alternative methods of discrimination. An important distinction is between targeted and non-targeted price discrimination. In broad terms, a network operator could select particular users or uses that it thinks should pay more for access and adopt policies that induce those firms to do so. For example, a network operator could set a higher price for all streaming video providers on the ground that such providers use a lot of platform capacity. The network could give other uses priority over the packets of any streaming video provider that fails to buy the higher level of access. Alternatively, the network could simply sell priority to whomever wants it, leaving each streaming video provider (or provider of any kind of any application) to decide for itself whether it is willing to have its packets delayed when there is congestion. The competitive risks vary for different kinds of targeted and non-targeted pricing.

Targeted and non-targeted pricing can also take several forms. A network operator could differentiate in its access pricing among specific users, particular kinds of use, or amounts of usage. The first, the targeting of specific users, would set prices depending on the identity of the provider whose traffic is moving over the network. Such categorization could simply be a proxy for use or usage. For example, if a network were to charge Acme Video, a hypothetical video-on-demand provider, a higher price for network access, it might do so not because Acme is Acme or because Acme provides video-on-demand, but because video-on-demand uses a lot of bandwidth and Acme happens to be a well-known provider that is easy to identify. On the other hand, the network operator might charge Acme the higher price either because

---

"free riding" on network infrastructure because they make big profits in which network owners do not share. The argument is weak. Applications providers are no more free riding on network platforms than vice versa. Consumers do not purchase Internet access from network operators just to cruise the network; they subscribe to reach on-line content and services. Just as network operators do not share in the profits of such applications providers, nor do they share their subscription revenues with the applications providers that consumers pay to reach. Moreover, it should be noted that many applications providers fail, and while network operators may not share in the profits of the successful ones, nor do they share the investment risk and losses from applications ventures that fail. What may look like free riding to the platforms may look like portfolio skimming from the other side.

Acme happens to be a rival in a particular complementary market or because the network operator knows Acme has deep pockets and will pay a lot not to have its traffic consigned to a slow lane. As discussed above, these latter two motivations may have little to do with cost recovery and carry some risk of anticompetitive harm or other allocative inefficiency.

Discrimination targeted at particular uses is potentially more neutral, although it is not necessarily better than discrimination by user. If higher prices are charged only based on whether a particular use is one that competes with a business of the network, then it may be anticompetitive. For discrimination by use to be better than discrimination by user, the categories must be chosen because they are reasonable proxies for costs imposed on the network rather than proxies for competition.

The most neutral of the three options for price discrimination is usage-based pricing, *i.e.*, charging for the amount of traffic an applications provider does or expects to put on the network. Some forms of usage-based pricing blur the line between targeted and non-targeted price discrimination. For example, if a network operator were to meter traffic and, as congestion developed, turn some capacity into a priority "lane" that any user could select for a fee, then the pricing would be non-targeted. If, however, the network operator mandated increasing fees as an applications provider crossed progressively higher thresholds of traffic volume, then the price discrimination would be targeting such high-volume users for higher access prices.

The most risky forms of price discrimination for competition and innovation, therefore, appear to be those where the network operator can target particular uses or users for higher prices. The least risky forms of price discrimination are those that charge for priority on a usage basis, where each applications provider can decide whether to purchase priority. While it may still be possible for pricing mechanisms to be designed to coerce particular applications providers to pay more, a posted menu of prices for priority based on usage raises many fewer concerns than targeted pricing based on use or user.

The costs and benefits of price discrimination by networks to applications providers thus vary with two sets of factors: the motivation for price discrimination and the method by which it is accomplished. Charging for priority in the presence of capacity constraints and congestion is more likely to yield benefits than is selling priority in the absence of capacity constraints. The first can represent an efficient response to scarcity; the second runs the greater risk of being an inefficient exercise of market power. Next, charging for priority based solely on usage rather than setting terms that target particular uses or users is more likely to avoid anticompetitive uses of price discrimination.

A basic taxonomy of network price discrimination, compared by level of anticompetitive risk, is summarized in the table below.

A Simple Taxonomy of Price Discrimination by Networks

	Targeted Pricing	**Non-Targeted Pricing**
Priority with Capacity Constraint	Moderate anticompetitive risk (??)	Lowest anticompetitive risk (best option)
Priority without Capacity Constraint	Highest anticompetitive risk (worst option)	Moderate anticompetitive risk (??)

The schema presented above suggests that not all discrimination need be equally harmful, in turn implying that the costs and benefits of network neutrality regulation will differ depending upon which kind of conduct it prohibits. To the extent there can be benefits to price discrimination itself, prohibiting even the comparably benign forms of discrimination might forego benefits in return for the prevention of less substantial harms. The next section addresses the implications of this possibility for regulatory policy.

C. Conclusion: Policy Alternatives Going Forward

The different motivations and methods of price discrimination raise the possibility of policy solutions that focus selectively on the most harmful kinds of discrimination without prohibiting other non-neutral conduct that could yield net benefits. Policy could regulate actions most likely to foreclose competition either among applications providers or between applications providers and the underlying network. Such regulation would not need to preemptively prohibit networks from offering a non-targeted menu of access tiers available to all applications providers regardless of their identity or type of service. This more selective focus is consistent with two commentators' recommendation for regulation that precludes network owners from discriminating among data packets routed on their networks based on the identity of users or uses.[30] It reduces the risks of targeted discrimination without banning discrimination altogether, thereby preserving some of the potential

30. *See* Brett Frischmann & Barbara van Schewick, *Yoo's Frame and What It Ignores: Network Neutrality and the Economics of an Information Superhighway*, 47 JURIMETRICS J. (forthcoming Summer 2007), *available at* http://ssrn.com/abstract=1014691.

benefits of upstream price discrimination by network operators. In terms of the chart displayed above, regulation would rule out the two left-hand quadrants. One might also try to rule out the lower right hand quadrant because the priority there is discretionary rather than driven by physical capacity constraints. Capacity constraints may be hard to observe and monitor, however, so regulation might as a practical matter do better to focus more on the method (*i.e.*, pricing structure) than on the motivation (*i.e.*, existence or not of real capacity constraint) for price discrimination.

There are different ways in which departures from non-targeted pricing, and the associated hazards for competition, could be regulated. One alternative is to have a basic rule that prohibits outright blocking of any (legal) applications provider, coupled with a regime of *ex post* enforcement against price discrimination that can be demonstrated to be anticompetitive. The approach here is primarily an antitrust-style approach. It has the virtue of not prohibiting much conduct in advance of proven anticompetitive effects, but would involve the courts and enforcement agency in assessing the detailed terms of each individual deal that came before them. The no-blocking rule would mean that such an *ex post* regime would differ from general U.S. antitrust law, which generally does not prohibit outright refusals to deal.[31] The focus of *ex post* enforcement would more likely be on whether the terms of trade were anticompetitive or not.

An alternative solution would be to impose some *ex ante* restraints on those terms of trade through a network-neutrality rule that imposes a light form of common carriage on the network operator. A modest rule might still allow networks to offer different access terms to applications providers but would require that those terms be transparent and available to all such providers. One promising proposal combines such an approach with *ex post* enforcement against any anticompetitive uses of price discrimination by a network.[32] The devil is likely to be in the details for either of these approaches, and detailed exploration is beyond the scope of this brief essay. The important point is that intermediate solutions exist that can dampen the worst potential harms of network access discrimination, without altogether banning all price-mediated prioritization of network traffic. In light of the open questions that each side of the debate raises, such intermediate solutions warrant further development.

Finally, the most essential long-run strategy to reduce the risks of anticompetitive discrimination raised by the advocates of network neutrality is to focus on horizontal competition rather than vertical

31. *See* Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP, 540 U.S. 398, 408-09 (2004).

32. ATKINSON & WEISER, *supra* note 4, at 12.

regulation. If the competitive progress of the U.S. telecommunications market can be maintained through effective radio-spectrum policy, network interconnection rules, and vigilant antitrust (particularly merger) enforcement, then network neutrality concerns will diminish. Congress and the FCC should, therefore, not lose track of longer-term structural solutions for improving competition and innovation in the broadband market, and should ensure that any interim regulation they impose will not remain in force as market conditions no longer justify them.

SHOULD COPYRIGHT OWNERS HAVE TO GIVE NOTICE OF THEIR USE OF TECHNICAL PROTECTION MEASURES?

PAMELA SAMUELSON & JASON SCHULTZ*

* Pamela Samuelson is the Richard M. Sherman Distinguished Professor of Law at the University of California Berkeley School of Law; Jason Schultz is a Staff Attorney at the Electronic Frontier Foundation.

INTRODUCTION

Advances in digital technologies have made many things possible, including cheap and easy copying and distribution of commercially valuable digital content, such as sound recordings and motion pictures, via global digital networks.[1] To counteract this easy copying, some copyright owners have adopted technical protection measures (or "TPMs", sometimes also referred to as "digital rights management" or "DRM" technologies) to control unauthorized access to and uses of digital content in mass-market products and services.[2] Copyright owners in the entertainment industry regard TPMs as essential to the creation of viable global markets for digital content.[3]

Consumers of digital products, however, often find TPMs frustrating, annoying, and harmful. TPMs may inhibit playful and creative uses of digital works and other non-infringing uses of the content, such as time- or platform-shifting. Consumers are especially likely to be frustrated and upset when they purchase technically restricted content without being given advance notice about what TPMs will disable or otherwise do that they do not expect. This article will demonstrate that many copyright owners are failing to give adequate and effective notice of TPM restrictions. This lack of transparency about TPMs has caused consumers several different kinds of harm. We believe that some regulatory action is necessary to address the notice problems that TPMs have brought about, and that this can be done without undermining the content protection goals that copyright owners have in using TPMs.

Part I of this article demonstrates that consumers have many expectations about what they should be able to do with digital content.

---

1. *See, e.g.*, NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 23-75 (Nat'l Academy of Sciences 2000) (discussing advances in digital technologies that have given rise to difficulties of enforcing copyright protections).

2. We will generally use the term "technical protection measures" and the acronym "TPM" to refer to technical locks that other commentators refer to as "digital rights management" or "DRM" technologies, except when we are quoting from sources that use the latter term. We regard TPM as a more neutral term than DRM that avoids resolving the ambiguity about whose "rights" matter in the context of DRM. *See, e.g.*, Pamela Samuelson, *Digital Rights Management {and, or, vs.} the Law*, COMM. ACM, Apr. 2003, at 41 (discussing the complex intersection of legal rights and technical measures).

3. *See, e.g.*, WORKING GROUP ON INTELLECTUAL PROP. RIGHTS, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 10-13 (1995) (expressing concern about infringements made possible by the Internet and digital technologies and the importance of technical measures to inhibit infringements). One British copyright lawyer has optimistically opined that "[t]he answer to the machine is in the machine." *See* Charles Clark, *The Answer to the Machine is the Machine*, *in* THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 139 (P. Bernt Hugenholtz ed., 1996).

In general, they expect to be able to do at least as much with digital content as they could with copies of copyrighted works in the traditional analog world; indeed, they often expect to be able to do even more with digital content than with analog works. When TPMs interfere with consumers' ability to engage in such uses, as many TPMs are programmed to do, consumers are likely to be frustrated and upset, especially if they purchased this product without notice of the restrictions.

Part II observes that many copyright owners who employ TPMs to protect digital content products do not give adequate and effective notice about technical restrictions on the usability of that digital content. Sometimes copyright owners give no notice at all about the technical restrictions, while other times, notice is inadequate or ineffective. Part II identifies six categories of harm that consumers have experienced as a result of the failure to give adequate and effective notice of TPM restrictions.

Part III discusses several studies and reports that have characterized the lack of notice of technical restrictions on digital content as a consumer protection issue warranting attention from policymakers. While European commentators have been more active in analyzing transparency and other consumer protection issues arising from TPM'd content, American policymakers and commentators are becoming more aware of these issues, particularly after the "magnificent disaster" of the Sony-BMG rootkit incident.[4]

Part IV considers several policy options for addressing the inadequacy of notice problem discussed in Parts II and III. The least interventionist strategy on the policy spectrum is to trust the market to produce an appropriate degree of notice of technical restrictions in digital content products and services. For reasons explained in Part IV, we are skeptical that the market has or will fix the notice problem with TPM'd content. The most interventionist strategy would not only require notice of technical restrictions but would also impose substantive restrictions on what digital content providers can do (and not do) with TPMs in restricting consumer uses of digital content.

In the middle of the policy spectrum lie alternatives that envision a role for the Federal Trade Commission ("FTC") in studying the notice problem with TPM'd content and developing standards for adequate and effective notice of TPM restrictions on digital content. This article recommends that the FTC should conduct a thorough empirical investigation of TPM'd digital content, with special attention to the adequacy and effectiveness of notice of technical restrictions, and should

4. Deirdre Mulligan & Aaron Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. (forthcoming 2007).

report to Congress about whether legislation to mandate notice is necessary to protect reasonable consumer expectations as to technically protected digital content.

I. CONSUMER EXPECTATIONS AS TO DIGITAL CONTENT AND TPMS

Consumer expectations about permissible uses of digital content have been shaped in part by personal use patterns arising from experiences with traditional media. After purchasing long-playing ("LP") recordings of musical works back in the olden days, for example, consumers felt free to make personal use copies to play on other platforms (e.g., making tapes of the LPs to play in their cars) or as backups in case the LPs got scratched.[5] When the commercial medium for recorded music shifted to compact discs ("CDs"), consumers similarly felt free to make personal use copies of the music (e.g., loading it onto the hard-drives of their computers). When Sony introduced Betamax video tape recorders into the market in the mid-1970's, purchasers used them to make time-shift copies of broadcast television programming, among other things.[6] Courts have generally regarded time-, space-, and platform-shifting to be fair uses of copyrighted works, seemingly conforming the law with consumer expectations.[7]

It is thus not surprising that consumers expect to be able to time-, place-, space-, and platform-shift as to digital media products, as well as to make backup copies.[8] Because digital technologies enable new

---

5. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, COPYRIGHT AND HOME COPYING: TECHNOLOGY CHALLENGES THE LAW 11-14 (1989), *available at* http://govinfo.library.unt.edu/ota/Ota_2/DATA/1989/8910.PDF (reporting on surveys about personal use copying).

6. *Id*. at 11-12.

7. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442-43 (1984) (time-shift copying of broadcast television programming is fair use); *In re* Aimster Copyright Litig., 334 F.3d 643, 652-53 (7th Cir. 2003) (noting space-shifting as a possible fair use); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1079 (9th Cir. 1999) (space-shift copying "is [a] paradigmatic noncommercial personal use."); S. REP. NO. 102-294, at 30 (1992) ("[t]he purpose of [the Audio Home Recording Act] is to ensure the right of consumers to make analog or digital audio recordings of copyrighted music for their private, noncommercial use."). *But see* A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 915-16 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001) (rejecting argument that space-shifting through use of Napster's network was a fair use for purposes of assessing whether Napster had or was capable of substantial non-infringing uses). The implications of *Sony* for various forms of personal use copying are explored in Pamela Samuelson, *The Generativity of* Sony v. Universal*: The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831 (2006).

8. *See, e.g.*, 17 U.S.C. § 117 (2000) (authorizing owners of software programs to make backup copies); Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 266-67 (5th Cir. 1988) (affirming the making of software backup copies as a non-infringing use of copyrighted materials); DigitalConsumer.org, Consumer Technology Bill of Rights, http://digitalconsumer.org/bill.html (last visited Nov. 1, 2007).

flexibilities in ways to use and consume digital information, consumers have come to expect to be able to do more with digital media products than they could do with analog media products.[9] Consumers may, for example, expect to be able to link works together, format-shift, annotate them, tinker with them, remix and mashup existing digital content, and share their new creations with others.[10]

The use of TPMs may impair personal uses that consumers expect to be able to make of digital content.[11] Copy-protected CDs, for example, may prevent platform-shifting and backup copying.[12] One cannot easily make backup copies of DVD movies because of TPMs.[13] DVD movies, moreover, may not be playable on all DVD devices, insofar as region-coding interferes with this ability.[14] Even technical sophisticates may have difficulty playing DVD movies on computers which use the Linux operating system.[15] "Ripping" movies from DVDs to store them on computer hard-drives or to make mashups or remixes can likewise be thwarted by TPMs.[16] Online music stores may use TPMs to prohibit personal use sharing of music.[17] Consumer experiences with online music stores have often been confusing and dismaying because of the mismatch between personal use expectations of users and what the services enable and disable through TPMs.[18]

---

9. *See, e.g.*, NATALI HELBERGER ET AL., DIGITAL RIGHTS MANAGEMENT AND CONSUMER ACCEPTABILITY: A MULTI-DISCIPLINARY DISCUSSION OF CONSUMER CONCERNS AND EXPECTATIONS 21 (2004), *available at* http://www.indicare.org/tiki-download_file.php?fileId=111 (giving examples of a wide array of personal uses that consumers expect to be able to make of digital media products).

10. *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

11. *See, e.g.*, Deirdre Mulligan, Aaron J. Burstein & John Han, *How DRM-based Content Delivery Systems Disrupt Expectations of 'Personal Use,'* PROC. OF THE 2003 ACM WORKSHOP ON DIGITAL RIGHTS MGMT. 77 (2003).

12. CTR. FOR DEMOCRACY & TECH., EVALUATING DRM: BUILDING A MARKETPLACE FOR THE CONVERGENT WORLD 7-8 (2006) [hereinafter CDT REPORT], *available at* http://www.cdt.org/copyright/20060907drm.pdf.

13. *Id.* at 4.

14. *See, e.g.*, *id.*; HELBERGER ET AL., *supra* note 9, at 21.

15. *See, e.g.*, Declan McCullough, *Teen Hacking Idol Hits Big Apple*, WIRED, July 20, 2000, http://www.wired.com/culture/lifestyle/news/2000/07/37650 (noting inability to play DVDs on Linux systems).

16. CDT REPORT, *supra* note 12, at 3. Yet, the widespread availability of DeCSS has enabled many consumers to be able to make mashups from DVD movies, notwithstanding the ruling in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (holding DeCSS to be an unlawful tool under U.S. anti-circumvention rules). *See* Posting of Fabienne Serriere to Engadget, How-To: Convert a DVD for Your iPod (with Video) in Windows, http://www.engadget.com/2005/10/14/how-to-convert-a-dvd-for-your-ipod-with-video-in-windows/ (Oct. 14, 2005).

17. CDT REPORT, *supra* note 12, at 9.

18. Mulligan et al., *supra* note 11; Ken Fisher, *Musicload: 75% of Customer Service Problems Caused by DRM*, ARS TECHNICAL, Mar. 18, 2007, http://arstechnica.com/news.ars/post/20070318-75-percent-customer-problems-caused-by-

Consumer expectations about flexible uses of digital content are, moreover, not static; they evolve as advances in digital technologies and user innovations open up new possibilities for use.[19] One recent report has observed that consumers want and expect "[f]lexible personal use—the ability to read, listen to, play, or watch a lawfully acquired work in a manner and sequence of the consumer's own choosing."[20] This report recommends that "[a]s much as possible, DRM solutions should seek to allow users to interact with, excerpt, and expand on existing works in ways that are consistent with copyright law,"[21] although it recognizes that TPM systems used in commercially distributed digital content are thus far "not well adapted to the task of facilitating end user creation."[22]

Consumers of digital media products have other legitimate expectations as well, including expectations that their privacy and security interests will be respected. In the analog world, it was almost never possible for authors, publishers, and other commercial distributors of content to monitor consumer usage of copyrighted works or to take actions that would make their customers insecure. Once a consumer bought a book, an LP, or a videocassette of a movie, he or she could take it home to read, listen to, or watch free from surveillance or control by the content's commercial distributors.[23] Consumers had no reason to fear that their use of these products in the privacy of their homes or offices would undermine their security from external attacks. Consumer expectations about privacy and security continue to be reasonable, but it has become technically possible for these expectations to be thwarted through the embedding of technical measures that monitor usage of digital media products and/or render users' computers vulnerable to attack.[24] TPMs may, moreover, cause other unanticipated negative impacts on consumers.[25]

II. CONSUMER HARMS RESULTING FROM THE LACK OF EFFECTIVE NOTICE OF TPM RESTRICTIONS

The disparity between consumer expectations about flexible uses of

---

drm.html (noting that "Deutsche Telekom's Musicload, one of the largest online music stores in Europe, has come out strongly against DRM on account of its effects on the marketplace and its customers").

19. CDT REPORT, supra note 12, at 14.

20. *Id.*

21. *Id.* at 17.

22. *Id.*

23. *See, e.g.*, Julie E. Cohen, *The Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace,* 28 CONN. L. REV. 981 (1996).

24. CDT REPORT, *supra* note 12, at 10.

25. *Id.* at 20 ("DRM may drain battery or processing power" or "modify[] the operation of . . . device drivers for DVD burners.").

digital media and limitations imposed by TPMs gives rise to significant tensions for the technology and entertainment marketplaces to mediate. Copyright owners may be aware that TPMs will not be popular with customers, and this creates incentives not to disclose their use in advance. When copyright owners or TPM vendors fail to adequately and effectively disclose the existence of the TPMs and the limits they impose, however, it exacerbates the tension mentioned above because the marketplace is operating on imperfect information.[26] The failure to give adequate and effective notice of TPM restrictions has resulted in six types of harms to the public: 1) lack of expected interoperability, 2) privacy intrusions, 3) security vulnerabilities, 4) anti-competitive lockouts, 5) risks of unforeseen anti-circumvention liability, and 6) unanticipated and unconsented to changes in or discontinuation of service.

A. Lack of Expected Interoperability

Among the most widespread concerns arising from use of TPM technology is the potential damage it can inflict on device and service interoperability. It is well documented that many of the advantages consumers enjoy from the digital networked economy result from compatibility between devices, formats, platforms, and applications.[27] These "network effects" increase the value of the overall network for each individual user. However, in order to maintain and exploit this value, devices and systems on the network must be sufficiently compatible to allow high quality data exchanges and high rates of information transfer at low transaction costs. TPMs, at their core, tend to be designed to thwart information transactions by erecting barriers to data exchange. Thus, the tension between TPMs and the value of

---

26. *Digital Media Consumer Rights Act of 2003: Hearing on H.R. 107 Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. 12 (2003) (testimony of Rep. Rick Boucher); *see also* 149 CONG. REC. S11571 (2003) (statement of Sen. Sam Brownback introducing S. 1621, titled the Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, to the Senate); Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, S. 1621, 108th Cong. § 2(2) (noting increased confusion among industry, educational institutions, libraries, and consumers as access controls become more prevalent in the marketplace); Julian Bajkowski, *Intel Quietly Adds DRM to New Chips*, DIGITAL ARTS, May 27, 2005, http://www.digitalartsonline.co.uk/news/index.cfm?NewsID=4915; Marc McEntegart, *No Pre-Owned Games to be Allowed for Playstation 3*, INQUIRER, Nov. 9, 2005, http://www.the-inquirer.com/default.aspx?article=27568.

27. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575 (2002); Mark A. Lemley, *The Law and Economics of Internet Norms* 29-30 (Berkeley Program in Law & Econ., Working Paper Series, Paper No. 132, 1999), *available at* http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1131&context=blewp (discussing positive influence of norms on Internet network effects).

interoperable networks has proven to be a long-standing one with significant implications for technology law and policy.

This tension is exacerbated when notice of TPM restrictions is inadequate or ineffective. For example, Apple, Inc. has designed its iTunes Music Store ("iTMS") and iPod music player with proprietary TPM technology so that songs from iTMS will only play on the iPod and not on other portable digital music devices. In addition, it has designed the iPod so that it will only accept music files from the iTunes store, or in various non-TPM formats such as MP3. For vendors of other music devices and other TPM-encoded music files, this presents a problem of interoperability. Users of iTMS and the iPod are precluded from interoperating with other digital music devices and vendors. Yet nowhere on Apple's website or on its products is there any indication to the purchaser of such restrictions or the exact limitations they impose.[28] This lack of notice, and the lack of interoperability the Apple TPM causes, has led to several public policy inquiries focused on consumer protection implications.[29]

In 2005, moreover, Sony BMG Music distributed thousands of sound recordings in CDs that contained TPM software designed to embed itself in the Windows Operating System where it could monitor and restrict use of the musical files from the CD.[30] While the CDs were labeled with a short "Copy Protected" notification, the notice did not clarify what this term meant, nor what uses were restricted and how. On the back of XCP protected CDs, there was a list of certain platforms on which one could play the music, but not which applications or devices would play them. The notice summarized the user's right to make backups or mixed playlists as "limited copies" without any explanation of how many copies, on what media, and what other computers would be able to play them.[31] Because of the inadequacies of this notice, users lacked sufficient information to understand the limits on interoperability

28. *See* Apple Inc., iTunes Store – Terms of Service, http://www.apple.com/legal/itunes/us/service.html (last visited Oct. 22, 2007) (noting that use of the iTMS requires "a compatible device" and may require the use of an "authorized digital player" but does not specify or define that term). *Compare* Apple Inc., iTunes Store – Terms of Sale, http://www.apple.com/legal/itunes/us/sales.html (last visited Oct. 22, 2007) (noting that in regard to iPod Games, the Games "are compatible only with 5th generation (video) iPods. The Games will not function on any other device, including your personal computer.").

29. *See* Stephen Withers, *Europe Continues to Push for iTunes Interoperability*, ITWIRE, Mar. 12, 2007, http://www.itwire.com.au/content/view/10368/53/; Jo Best, *Law to Make iTunes Compatible with Microsoft?*, SILICON.COM, Apr. 7, 2005, http://management.silicon.com/government/0,39024677,39129365,00.htm.

30. *See* Mulligan & Perzanowski, *supra* note 4; Electronic Frontier Foundation, A Spotter's Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Oct. 22, 2007).

31. Electronic Frontier Foundation, A Spotter's Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Oct. 22, 2007).

that Sony BMG had imposed upon them with its XCP protected CDs.

Technical restrictions like these often surprise, frustrate, and confuse consumers, especially when they are applied to media such as CDs that consumers have come to expect to be available without such limits. TPMs may place unwarranted burdens not only on consumers, but also on retailers and manufacturers of computers or consumer electronics devices. This is because consumers may complain to the retailers or manufacturers about their frustrations with TPM products or services. It is often not obvious to the complaining consumers that the technical restriction was imposed by the maker of the digital media product or service, not the manufacturer or seller of the equipment on which consumers choose to render the digital media product or service.

A third example of TPM-induced non-interoperability is DVD region codes. Under the technological system designed by the DVD Copy Control Association, the industry coalition that controls the standards for DVD production and playback, DVDs are often encoded with a numerical identifier that corresponds to a specific geographic region in which the DVD is authorized to be distributed. If, for example, someone purchased a DVD with a European Region Code (Region 2) while on vacation in France, he or she could not play that DVD on most U.S. manufactured DVD players because they are encoded to play only DVDs having a U.S. Region Code (Region 1). Notwithstanding the pervasiveness of DVDs, most DVDs do not disclose region code restrictions to consumers, either at the point of sale, or in the accompanying literature for the DVD. Consumers who travel or move from one region to another risk unfair surprise in finding that media they have legitimately purchased does not work with equipment in their hotel or new home.[32] Without proper notice, consumers may believe that this is a problem with the DVD they bought or with their DVD player instead of a TPM restriction imposed on them by the copyright holder in conjunction with the DVD Copy Control Association.

TPM-induced non-interoperability problems are not limited to digital content. Hewlett-Packard, for example, has started "region coding" its printers and printer cartridges so that consumers must buy the latter in the same region of the world as they bought the printer.[33] If the "wrong" cartridge is inserted, HP equipment will not print documents, even though the cartridge is, except for the difference in the region code,

32. A similar problem exists within the iTunes Music Store TPMs. Apple has reportedly been using TPMs to limit access to particular music files based on a user's country of origin without adequate and effective notice to users of these limitations. *See* Paul Collins, *iTunes: The Insanely Great Songs Apple Won't Let You Hear*, SLATE, Jan. 23, 2007, http://www.slate.com/id/2158151/.

33. David Pringle & Steve Stecklow, *Electronics With Borders: Some Work Only in the U.S.*, WALL ST. J., Jan. 17, 2005, at B1.

functionally identical to the "right" region-coded cartridge.[34]

B. Privacy Invasions

Some TPM-protected products and services have been designed to monitor consumer usage and report back about it to the owners of copyrights in the TPM-protected works or to their agents. This monitoring often happens at a very deep technical level of the consumer device or product. Ordinary consumers are unlikely to be aware of the existence or extent of such monitoring or of uses that may be made of personal data collected through such monitoring.[35] This poses the harm of invading users' privacy interests and exposing them to unwanted surveillance or profiling.

Blizzard Entertainment, for example, has deployed a privacy-intrusive TPM in software associated with its very popular online videogame called "World of Warcraft"[36] in which millions of users log in to Blizzard's servers and interact. Blizzard conceived of this privacy-invasive TPM as a strategy for controlling cheating and "hacks." An "update" of its software included a TPM monitor called "The Warden," which users installed on their personal machines.[37] The Warden TPM monitored each user's computer, including any active window, to make sure no unauthorized programs were running while the game was in play.[38] Upon detecting any such program, The Warden was designed to investigate the user's gaming activities; based on the results of the investigation, Blizzard may take steps including suspending the user's account.[39]

While some users did not object to the Warden because it kept some players from cheating in the game, others were upset by the failure of Blizzard to disclose the privacy implications of the TPM, which included sometimes scanning email addresses and website URLs.[40] While Blizzard does disclose some general information about The Warden in its

---

34. *Id.*

35. *See* Bajkowski, *supra* note 26; *see also* CANADIAN INTERNET POLICY AND PUBLIC INT. CLINIC, DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES AND CONSUMER PRIVACY (2007), *available at* http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf.

36. World of Warcraft, http://www.worldofwarcraft.com (last visited Oct. 22, 2007).

37. Mark Ward, *Warcraft Game Maker in Spying Row*, BBC NEWS, Oct. 31, 2005, http://news.bbc.co.uk/1/hi/technology/4385050.stm.

38. Jon Espenschied, *No Security Reprieve from Blizzard's Warden: Two Good Reasons to Pass on MMORPGs in the Office*, COMPUTERWORLD, May 13, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019240; Schneier on Security, Blizzard Entertainment Uses Spyware to Verify EULA Compliance, http://www.schneier.com/blog/archives/2005/10/blizzard_entert.html (Oct. 13, 2005).

39. *Id.*

40. *Id.*

End-User License Agreement, there are very few specifics about how and what programs are restricted from running and what information is actually collected and/or sent back to Blizzard.[41]

Similar concerns about TPM privacy invasiveness were lodged against Sony BMG after it became known that its TPM system for copy-protecting CDs sent information about consumer usage over the Internet back to the company that made the TPM for Sony[42] and against the now-defunct Digital Video Express (Divx) system, which reportedly collected information on every movie a user would watch.[43]

Copyright owners have incentives to embed privacy-invasive monitoring and reporting features in their TPMs. As with the Blizzard software, monitors can aid in the detection of infringing copies of copyrighted works; they can also facilitate price discrimination and profiling about customers that will allow rights holders to offer new products and services to them or to sell user profiles to other firms. If experience thus far is any guide, deployers of TPM monitoring software are unlikely to give adequate and effective notice of the monitoring capabilities and what the monitoring firm plans to do with the information collected by the TPM system. We worry that that the privacy-invasive TPMs of the present may augur further such systems in the future.[44] We believe that firms that distribute digital media products or services that monitor consumer uses should be required to give their customers effective notice of any such monitoring and of uses that they intend to make of such data. Fair information practices should also be followed in collecting and processing of such data.[45]

C. Security Vulnerabilities

Certain kinds of TPMs may also make consumers' computers

---

41. World of Warcraft, End User License Agreement § 5 http://www.worldofwarcraft.com/legal/eula.html (last visited Oct. 22, 2007).

42. Posting of J. Alex Halderman to Freedom to Tinker, Sony Shipping Spyware from SunnComm, Too, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005).

43. Dan Fost, *Divx's Death Pleases Opponents*, S.F. CHRON., June 18, 1999, *available at* http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/06/18/BU89741.DTL.

44. *See generally* Lee A. Bygrave, *Digital Rights Management and Privacy - Legal Aspects in the European Union in* DIGITAL RIGHTS MANAGEMENT - TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 418 (Eberhard Becker et al. eds., 2003); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003); Ian Kerr & Jane Bailey, *The Implications of Digital Rights Management for Privacy and Freedom of Expression*, 2 J. INFO. COMM. & ETHICS SOC'Y 87 (2004).

45. *See generally* ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO INTELLECTUAL PROPERTY RIGHTS (2005), *available at*, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf (noting "an increasing gap between the protection of individuals in the off-line and on-line worlds, especially considering the generalised tracing and profiling of individuals").

vulnerable to security problems. When TPMs exert control over computers and other devices to limit access or functionality to users, they are, in essence, technically overriding the users' default configurations and decisions about how to operate their technology.[46] Anticipating that some users with technical skills may try to disable TPMs, TPM makers have developed ways to make the TPMs "resistant" to user tampering or to hide the TPM software so that the user cannot locate or disable the TPM. This design approach, however, is likely to make users' computers vulnerable to certain kinds of unanticipated exploitations. Makers of malicious software, such as viruses, spyware, or spam-generating programs, for example, can take advantage of certain attributes of TPM "resistant" design to hide their own programs from the user or to thwart the user's ability to seek out and remove dangerous files from their systems.

In order to avoid detection (and subsequent removal) by users, for example, the Sony BMG XCP TPM used a well-known computer exploit technique called "a rootkit" to hide itself in the registry files of the Windows operating system by pretending to be one of the thousands of essential components that Windows needs to operate correctly.[47] The XCP software was designed to evade most attempts to detect it so it could monitor use of the digital music files on the Sony BMG CDs without interference from the user. However, because of certain design flaws, the XCP software made users' computers susceptible to being taken over by malicious programs. The malicious programs were able to use XCP's evasion feature to avoid detection by anti-virus and anti-spyware programs typically installed on computers running Windows. This malicious software could then, in turn, be used to infect the host computer when the Sony BMG CD had been inserted and spread itself undetected to other computers via network connections.

By failing to disclose—and, in fact, actively concealing—the existence of the XCP TPM, Sony not only misled its customers about restrictions on the usability of the copyrighted content they had purchased, but also exposed them to significantly increased risks of malicious software undermining computer security. Adequate and effective disclosure of these risks would not have necessarily prevented the full extent of the harm consumers suffered, but it would certainly have helped cautious consumers avoid installing the software in the first instance. We fear that this example may be just the beginning of a

46. *See, e.g.*, SETH SCHOEN, ELEC. FRONTIER FOUND., TRUSTED COMPUTING: PROMISE AND RISK 1, http://www.eff.org/files/20031001_tc.pdf (noting that while "trusted computing" technologies solve some of today's electronic security problems, they may do so "while giving third parties the power to enforce policies on users' computers against the users' wishes").

47. *See* Mulligan & Perzanowski, *supra* note 4.

pattern of security-related problems for users of TPM technology.[48]

D. Anti-Competitive Lock-out

TPMs can also be designed to prevent users from using non-infringing competing products as alternatives to those provided by the TPM content developer or from using independent service vendors other than those affiliated with or licensed by the original TPM-encoded product or service. Consumers suffer harm when TPMs are used to lock-out competitive products and services, especially when they were given no notice of the existence of the lockout system before purchasing the product or service.

An example is the case of *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*,[49] in which the maker of a garage door opener ("GDO") asserted that a competitive GDO manufacturer could not lawfully distribute its GDOs because they bypassed an access control feature of Chamberlain's GDOs in violation of the Digital Millennium Copyright Act ("DMCA") anti-circumvention rules, now codified as Section 1201 of Title 17 of the U.S. Code.[50] Chamberlain had installed a set of rolling codes that were synchronized between the remotes and the openers. It asserted that these rolling codes were access controls protecting its copyrighted software running inside the GDO, and by bypassing the access controls, it was illegal under the DMCA.

One of the problems the court perceived with Chamberlain's DMCA claim was that Chamberlain had failed to disclose this technological lock-out feature to its customers when they purchased its GDOs.[51] It was, ironically, only after an after-market GDO remote competitor, Skylink, reverse-engineered Chamberlain's programs and offered a competing universal GDO remote that Chamberlain disclosed the existence of the TPM via the lawsuit it filed against Skylink under Section 1201.

Use of TPMs as lock-out devices significantly raises switching costs for consumers, creates inefficiencies in the marketplace for such technologies, and puts consumers at risk of being stuck with inadequate or debilitating purchases. Other examples of TPMs being used as lock-out mechanisms have arisen in the context of printers and printer ink

48. *See, e.g.*, John Leyden, *Trojans Exploit Windows DRM Loophole*, REG., Jan. 13, 2005, http://www.theregister.co.uk/2005/01/13/drm_trojan/ (reporting that "Trojans and other malware" are able to subvert DRM features in Windows Media Player).

49. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

50. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 and 28 U.S.C. (2006)).

51. *Chamberlain Group*, 381 F.3d at 1187, 1194.

cartridges,[52] magnetic tape library storage systems,[53] car repair diagnostic software,[54] online videogame servers[55] and digital camera film files.[56]

E. Risks of Inadvertent Anti-Circumvention Liability

Inadequate notice of TPMs can also put consumers at risk of inadvertent anti-circumvention liability. There are unquestionably some situations in which people have been aware that copyright owners are using TPMs to protect their works, and hence, presumptively aware that Section 1201 of the DMCA protects rights holders against circumvention of these TPMs. The journalist Eric Corley, for example, was well aware that the DVD Copy Control Association required makers of DVD movies and DVD players to use the Content Scramble System ("CSS") TPM to protect DVD movies from unauthorized copying; Corley also knew that he was running the risk of legal liability under Section 1201 when he posted the source and object code of a program that bypassed CSS on the website of his online magazine.[57]

However, the history of DMCA enforcement efforts thus far suggests that there are significant gray areas as to anti-circumvention liability.[58] Some customers and competitors have been surprised to find themselves charged with Section 1201 violations, in part because the copyright owner did not give adequate or effective notice that it was using a TPM that was subject to Section 1201 strictures.

Consider, for example, the unwelcome surprise experienced by the

---

52. *See, e.g.,* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 528-32 (6th Cir. 2004).

53. *See, e.g.*, Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

54. *See, e.g.*, Auto Inspection Servs., Inc. v. Flint Auto Auction, Inc., No. 06-15100, 2007 WL 674312 (E.D. Mich. Feb. 28, 2007).

55. *See, e.g.*, Davidson & Assoc., Inc. v. Internet Gateway, Inc., 334 F. Supp. 2d 1164, 1167 (E.D. Mo. 2004), *aff'd sub nom.* Davidson & Assoc. v. Jung, 422 F.3d 630 (8th Cir. 2005) (using undisclosed TPM to lock videogames into vendor's proprietary servers); The Grip Line Weblog by Ed Foster, Steaming about DRM, http://www.infoworld.com/weblog/foster/2005/01/04.html (Jan. 4, 2005) (describing videogame company Valve Software's attempt to restrict use of videogame to a single computer using undisclosed TPM).

56. *See Nikon Responds to RAW WB Concerns*, DIGITAL PHOTOGRAPHY REV., Apr. 22, 2005, http://www.dpreview.com/news/0504/05042203nikonnefresponse.asp (discussing allegations that Nikon encrypts certain "white balance" data when a user takes a picture with its camera but does not allow that data to be transferred when the user converts the RAW image file to a competing format).

57. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 324 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (affirming a lower court ruling that Corley was liable for violating Section 1201 of the DMCA by posting DeCSS on his website and linking to sites where DeCSS could be found).

58. *See generally* R. Anthony Reise, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003).

maker of chips designed for use in Lexmark-compatible printer cartridges when Lexmark sued it for violating Section 1201 in the *Lexmark International, Inc. v. Static Control Components, Inc.*, case.[59] Lexmark claimed that Static Control trafficked in unlawful circumvention technologies because its chips contained software that activated printer engine software code inside Lexmark printers, thereby bypassing a TPM that Lexmark had embedded in its software to control access to its copyrighted program.[60] The lower court found Lexmark's logic persuasive and enjoined Static Control from further manufacture of the Lexmark-compatible chips. This ruling was eventually overturned on appeal in part because the court decided that Lexmark had, among other things, failed to "effectively control[] access" to the printer program (for example, by encrypting it).[61] While we think the appellate court reached the right conclusion on 1201 liability, perhaps it should also have considered that Static Control had no reason to anticipate that Lexmark was using a 1201-relevant TPM to protect its printer program, let alone that it would charge Static Controls with 1201 violations for making chips for use in competing cartridges. It is also worth noting that while this case concerned the anti-trafficking provision of 1201(a)(2), Lexmark's conception of 1201 liability would logically lead to holding purchasers of Lexmark-compatible cartridges equally liable for violating this law, even though customers could not have reasonably anticipated being charged with violating Section 1201 based on their purchase of products that competed with Lexmark products.[62]

Lack of adequate notice of potential anti-circumvention liability was also a problem in *Chamberlain v. Skylink*.[63] Chamberlain's theory of liability was premised on the notion that since GDOs ran a software program when the remote activated it, the rolling code used by its GDO was a TPM that controlled access to that program and was circumvented by the defendant's remote. In both the lower court and at the appellate level, the judges reviewing the case expressed serious concerns over what the TPM at issue was and how the DMCA applied to it. What did it mean to "access" the software program at issue? What did the program protect? Was opening the garage door an unauthorized access of a

59. Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003), *vacated*, 387 F.3d 522 (6th Cir. 2004).

60. *See Lexmark*, 253 F. Supp. 2d at 947-57.

61. *Lexmark*, 387 F.3d at 551-53 (Merritt, J., concurring) (asserting that Section 1201 claims should not be used to block competition in the products market; the majority ruled only that Lexmark had not made a valid claim on the facts before them).

62. If the Static Control chip was an anti-circumvention tool, then users of printer cartridges embodying this chip would logically be in violation of 17 U.S.C. § 1201(a)(1)(A), which forbids bypassing TPMs that control access to protected works.

63. *Chamberlain Group*, 381 F.3d 1178.

copyrighted work (the software program) even though the user might be completely unaware of the program's existence? The Federal Circuit Court of Appeals eventually ruled that because there was no "nexus" between the user's actions and any potential copyright infringement, there was no Section 1201 violation, but the opinion suggests that issues of notice and fundamental unfairness supported its reasoning for limiting the DMCA's application in this case.[64]

Nor could Princeton Computer Science Professor Ed Felten have reasonably anticipated being charged with violating Section 1201 by the Recording Industry Association of America ("RIAA") when he and his students wrote a paper for presentation at a scientific conference based on their experience undertaking an RIAA-authorized challenge to "crack" recently developed TPMs for recorded music files.[65] RIAA claimed that if Felten et al. published their results, they would be trafficking in a circumvention device under Section 1201.[66] Felten filed for a declaratory judgment that presenting this paper would not violate the anti-circumvention laws, following which the RIAA mooted the suit. However, this threatened lawsuit created uncertainty about whether and to what extent future scientific research might be considered a violation of the DMCA.[67]

Consider also the case of *Davidson & Associates v. Jung*, in which the parent company of Blizzard Entertainment sued a group of open source developers for creating an interoperable game server (called the "BNETD" server) which allowed them to play Blizzard's Warcraft, Starcraft, and Diablo videogames.[68] In creating the BNETD server, the programmers deliberately avoided use of Blizzard's encryption protocols or authentication mechanisms that the client tried to send to the server in the hope that this would avert Section 1201 liability. However, both the district court and the appellate court found that, notwithstanding this intent, the developers had, in fact, made themselves liable under 1201 because their program did not respond to the encrypted data appropriately. The data, as it turns out, contained a unique serial number intended to prevent unauthorized copying. By ignoring this information, even in good faith, the courts found the developers were circumventing

64. *Id.* at 1203-04.

65. *See generally* Transcript of Motions, Felten v. RIAA., No. 01-CV-2669 (D.N.J. Nov. 28, 2001), *available at* http://w2.eff.org/IP/DMCA/Felten_v_RIAA/20011128_hearing_transcript.pdf.

66. *See* Letter from Matthew J. Oppenheim, Esq., RIAA Counsel, to Professor Edward Felton (Apr. 9, 2001), *available at* http://cryptome.org/sdmi-attack.htm.

67. *See* Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 SCIENCE 2028, 2028-30 (2001) (discussing the chilling effects of this threatened lawsuit on security researchers).

68. Davidson & Assoc. v. Jung, 422 F.3d 630 (8th Cir. 2005).

Blizzard's TPM and were thus liable even though they had no intention of furthering infringement of Blizzard games. Notably, there was no indication in the Blizzard End User License Agreement or Terms of Use that this TPM existed or what limitations, either technologically or legally, it was meant to impose.

Yet another example of potential inadvertent anti-circumvention liability attributable to inadequate TPM notices arose as to Sony's Aibo robotic dog. Sony released this programmable pet into the marketplace in 1999. Soon thereafter, an enterprising group of Aibo dog enthusiasts reverse-engineered the Aibo code and discovered how to write new programs to run on the Aibo system so that the dog could be directed to do any number of creative (albeit unauthorized by Sony) maneuvers, e.g., jazz-inspired dance sequences.[69] In 2001, Sony sent a cease-and-desist letter to the developers of a website called "aibohack.com" demanding that it stop distributing code that was retrieved by bypassing the copy prevention mechanisms of the robot.[70] After its customers strongly protested against this, Sony backed off from this position and allowed non-commercial reprogramming of the robot by its customers; however, the lack of clarity surrounding the limits of the Aibo TPM and the attendant legal risks are notable.

Techmo v. Ninja Hacker is a sixth example of unintentional legal exposure resulting from inadequate TPM notice.[71] Techmo sued the users and host of a forum where players of popular Techmo games traded "skins," graphical outfits used by the players in the games to designate skin color, uniforms, and other attire. In its complaint, Techmo alleged that in order to access and modify the skins, users needed to modify their Microsoft Xbox systems to allow interaction with an external computer hard drive. According to Techmo, this "unauthorized access" circumvented the protections on the game and violated Section 1201. Because the case settled soon after filing, there is no way to know how a court would have ruled on the legal merits of this claim, but it is fair to surmise that neither the users nor the host of the forum had adequate notice that Techmo was using the Xbox hardware as a TPM to restrict access to its game skins.

F. Changing Terms and Discontinued Service

Additional harms to consumers from inadequate notice of TPMs occur when consumers discover to their dismay that TPM-protected

69. *See Sony Uses DMCA to Shut Down Aibo Hack Website*, SLASHDOT, Oct. 27, 2001, http://yro.slashdot.org/article.pl?sid=01/10/28/005233.

70. *Id.*

71. *See* Kevin Poulsen, *Hackers Sued for Tinkering with Xbox Games*, SECURITYFOCUS, Feb. 9, 2005, http://www.securityfocus.com/news/10466.

products or services they have purchased have been programmed to enable alteration of functionality without giving them notice of the changes or an opportunity to object or to obtain a remedy for the lessened value of the altered product or service.

For example, in 2003, Intuit offered an activation feature to purchasers of its popular TurboTax software product that required users to register the product with a specific computer prior to activation.[72] Once registered, the software refused to let the user print their tax return or file it with the IRS electronically from any other computer without the purchase of another license or reactivation of the software.[73] Needless to say, this caused severe frustration for consumers who were not aware of the feature when they purchased the software product.

Apple Computer has instituted similar practices in its iTMS DRM, changing the number of copies and accessible computers available to past, present, and future users at least three times since they launched the service in 2001. In the iTunes Store Terms of Service, Apple expressly reserves the right to change the "Usage Rules" and other limits on the music purchased from the service at any time without prior notice to consumers.[74] Similar changes in service and features have occurred with personal video recorder manufacturers like TiVo as a result of deals these companies have made with TPM providers like Macrovision and content providers like HBO.[75]

Even more troublesome are situations in which companies that have tethered their content with TPMs discontinue service or go out of business. For example, when the DivX video disc system was available, one could purchase access to various movie titles for limited periods of time, such as 48 hours. One could also purchase "lifetime" access for significantly more money. However when the company that ran DivX went out of business,[76] it was unclear what would happen to those "lifetime" purchases. Would they be honored? Or would consumers lose access beyond the lifetime of the company?

---

72. *See* Cade Metz, *Intuit's TurboTax Activation Scheme Irks Users*, PCMAG, Jan. 10, 2003, http://www.pcmag.com/article2/0,1895,821308,00.asp.

73. *Id.*; *see also* The Gripe Line Weblog by Ed Foster, Steaming About DRM, http://www.infoworld.com/weblog/foster/2005/01/04.html (Jan. 4, 2005) (noting personal problems activating Christmas video game gift for his eight-year-old son).

74. *See* Apple Inc., iTunes Store – Terms of Service, http://www.apple.com/legal/itunes/us/service.html (last visited Oct. 20, 2007). Notably, at least one European Consumer Ombudsman has objected to this practice. *See iTunes Violates Norwegian Law*, FORBRUKEROMBUDET, June 7, 2006, http://www.forbrukerombudet.no/index.gan?id=11032467&subid=0.

75. Lucas Graves, *Has TiVo Forsaken Us?*, WIRED, Nov. 2004, http://www.wired.com/wired/archive/12.11/view.html?pg=3.

76. *See, e.g.*, Stephanie Miles, *Behind the Death of DivX Were Angry Customers*, CNET NEWS.COM, June 17, 1999, http://news.com.com/2100-1040-227248.html.

A similar situation recently arose involving Sony BMG's "Sony Connect" service. When the service launched in 2006, it included TPMs that monitored user usage to ensure compliance with certain rules about access and availability of songs. However, there was recently a news report suggesting that Sony would be shutting down the service, potentially leaving thousands of music fans and customers without access to the content they have legitimately downloaded.[77] Other subscription services such as Rhapsody and Napster raise the same issues about what will happen to consumers' access to TPM'd content if the company goes out of business or otherwise decides to shut the service down.

III. THE TPM NOTICE PROBLEM HAS BEEN NOTICED

Several European reports have emphasized the need for transparency when technical restrictions are embedded in mass-marketed digital content.[78] An especially thorough report on transparency and other consumer protection issues posed by TPM'd digital content is a report entitled "Digital Rights Management and Consumer Acceptability: A Multi-Disciplinary Discussion of Consumer Concerns and Expectations," published by a multi-institutional study group known as "The Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe" ("INDICARE").[79] The INDICARE Report considers five major categories of consumer protection concerns posed by these technologies: "(1) fair conditions of use and access to digital content, (2) privacy, (3) interoperability, (4) transparency and (5) various aspects of consumer friendliness."[80] This report discusses several EU directives that have a bearing on disclosure of TPM restrictions,[81] as well

77. *See* Rafat Ali, *Sony Connect to Close Music/Video Services; Focus on Servicing Playstation Group; 20 People to Go*, PAIDCONTENT.ORG, June 16, 2007, http://www.paidcontent.org/entry/419-sony-connect-to-close-music-video-services-focus-on-servicing-playstati/; *see also* Virgin.com, Sorry - Virgin Digital Has Now Closed!, http://www.virgindigital.co.uk/Message.aspx (last visited Oct. 22, 2007) (announcing discontinuation of DRM-based music downloading service without clear guidance for how users who have purchased music can continue to listen to those songs).

78. *See, e.g.*, ALL PARTY PARLIAMENTARY INTERNET GROUP, DIGITAL RIGHTS MANAGEMENT (2006), *available at* http://www.apcomms.org.uk/apig/current-activities/apig-inquiry-into-digital-rights-management/DRMreport.pdf [hereinafter APIG REPORT]; EUROPEAN CONSUMER LAW GROUP, COPYRIGHT LAW AND CONSUMER PROTECTION (2005), *available at* http://www.europeanconsumerlawgroup.org/Content/Default.asp?PageID=488 (follow 'Copyright Law and Consumer Protection, ECLG/035/2005' hyperlink) [hereinafter ECLG REPORT]; HER MAJESTY'S STATIONARY OFFICE, GOWERS REVIEW OF INTELLECTUAL PROPERTY (2006), *available at* http://www.hm-treasury.gov.uk/media/6/E/pbr06_gowers_report_755.pdf [hereinafter GOWERS REPORT].

79. HELBERGER ET AL., *supra* note 9.

80. *Id.* at vi.

81. *See id.* at 51-55.

as German legislation and French case law that require content owners to give consumers adequate notice about TPM restrictions.[82]

Another European report on DRM technologies was issued in the UK by the All Party Parliamentary Internet Group ("APIG"); it states that the group had reached "considerable consensus on the principle that consumers should be aware of what they are purchasing."[83] More specifically, there was agreement that "all [copy-protected] CDs should in the future come with a prominent label saying, 'you are not permitted to make any copies of this CD for any reason.'"[84] Full disclosure should also be given, says APIG, if technically protected CDs will not play on all devices, will not be playable if the user's device breaks or is stolen, and will record identity information about users.[85] It went on to recommend that the British Office of Fair Trading ("OFT") "bring forward appropriate labeling regulations so that it will become crystal clear to consumers what they will and will not be able to do with digital content that they purchase."[86] A second British report, Gowers Review of Intellectual Property, similarly recommended labeling of technically restricted digital content to protect legitimate consumer interests and expressed concern about the risks that TPMs could be used for socially undesirable purposes.[87]

The first American policy initiative aimed at addressing consumer concerns about inadequacy of notice as to TPM-protected copyrighted works was Congressman Rick Boucher's bill, H.R. 107, introduced in January 2003, which would have amended the FTC Act to give the agency authority to regulate labeling of copy-protected CDs of recorded music.[88] Among its proposed findings was that the introduction of copy-protected CDs "has caused consumer confusion and placed increased, unwarranted burdens on retailers, consumer electronics manufacturers, and personal computer manufacturers responding to consumer complaints."[89] If the recording industry was going to use copy-protection systems for CDs, it needed to be "responsible for providing adequate notice to consumers about restrictions on the playability and recordability of 'copy-protected compact discs.'"[90] The bill proposed to authorize the FTC to develop standards for appropriate labeling of such

82. *See id*. at 53 (discussing German labeling requirement for TPM'd content).
83. APIG REPORT, *supra* note 78, at 15.
84. *Id.* at 16.
85. *Id*.
86. *Id.* at 17.
87. *See* GOWERS REPORT, *supra* note 78, at 7 (noting in Recommendation 16 the need for a DRM systems labelling convention).
88. Digital Media Consumers' Rights Act of 2003, H.R. 107, 108th Cong. § 3 [hereinafter Boucher Bill].
89. *Id.* § 2(1).
90. *Id.* § 2(2).

CDs.[91] After promulgation of these standards, recording companies would be required to comply with those standards.[92] Thereafter, it would be an unfair trade practice for firms to introduce into the market unlabeled or mislabeled copy-protected CDs or to advertise such CDs unless the copy-protection feature was disclosed.[93] The bill would have also required the FTC to submit a report to Congress about the effects of the legislation.[94]

Senators Brownback and Wyden introduced similar legislation, although their bills were more general in addressing disclosure issues as to technically protected digital media products.[95] The Brownback bill would have authorized the FTC to establish an advisory committee to inform the Commission "about the ways in which access control technology . . . may affect consumer, educational institution, and library use of digital media products based on their legal and customary uses of such products," as well as about consumer awareness about the use of such technologies in digital media products.[96]

A year after the effective date of the legislation, the Brownback bill would have charged the FTC with promulgating regulations to require notice about technically protected digital media products unless their makers had "established [and implemented] voluntary rules for notice and labeling of access controlled or redistribution controlled digital media products," insofar as these technologies would affect the "legal, expected, and customary uses" of these products.[97] Thereafter it would be illegal to sell technically restricted digital media products without "clear and conspicuous notice" that "identifies any restrictions the access control technology or redistribution control technology used in or with that digital media product [a]s intended or reasonably could be foreseen to have on the consumers', educational institutions', or libraries' use of the product."[98] The FTC would also be required to report to Congress on the deployment of technically protected digital media products, on the extent to which such products allow customers to engage in lawful uses, and the extent to which notices of technical restrictions are effective.[99]

The Wyden bill had the same goal as the Brownback bill—to give

---

91. *See id.* § 3(d)(2)(A) (proposing to amend § 24 of the FTC Act to include "appropriate labeling requirements applicable to [certain] new audio discs").

92. *See id.* § 3(b)(1)–(2).

93. *See id.*

94. Boucher Bill, *supra* note 88, at § 4.

95. Digital Consumer Right to Know Act, S. 692, 108th Cong. (2003) [hereinafter Wyden Bill]; Consumers, Schools, and Libraries Digital Rights Management Awareness Act of 2003, S. 1621, 108th Cong. [hereinafter Brownback Bill].

96. Brownback Bill , *supra* note 95, at § 4(a).

97. *Id.* § 4(d).

98. *Id.* § 4(c).

99. *Id.* § 7.

consumers effective notice about technical restrictions built into digital media products—but had a broader perspective on the use of TPMs and sought to accomplish the goal somewhat differently. It recognized that media firms were embedding TPMs in digital media products in order to protect these products from illegal copying and that deployment of TPMs "could help promote a competitive digital marketplace in which consumers have a broad range of choices and media businesses can pursue a variety of business models."[100] However, it also recognized the legitimacy of consumer expectations about their ability to use and manipulate digital content "for reasonable, personal, and noncommercial purposes."[101]

The Wyden bill identified three significant risks posed by deployment of TPMs in digital media products: (1) that TPMs "could have the side effect of restricting consumers' flexibility to use and manipulate such content for reasonable, personal, and noncommercial purposes," (2) that use of TPMs "could unfairly surprise consumers by frustrating their expectations concerning how they may use and manipulate digital content they have legally acquired," and (3) that deployment of TPMs "could result in greater market power for the holders of exclusive rights and reduce competition, by limiting the ability of unaffiliated entities to engage in the lawful secondhand sale or distribution of such content."[102]

To guard against unfair surprise, the Wyden bill called for the FTC to develop rules to implement the following disclosure requirement:

> If a producer or distributor of copyrighted digital content sells such content or access to such content subject to technological features that limit the practical ability of the purchaser to play, copy, transmit, or transfer such content on, to, or between devices or classes of devices that consumers commonly use with respect to that type of content, the producer or distributor shall disclose the nature of such limitations to the purchaser in a clear and conspicuous manner prior to such sale.[103]

The bill proposed to authorize the FTC to "prescribe different manners of disclosure for different types of content and different distribution channels,"[104] and also to make exceptions to the notice requirement as to uses of TPMs "that are sufficiently unusual or uncommon that the burdens of prior disclosure would outweigh the

100. Wyden Bill, *supra* note 95, at § 2(a)(2)-(3).
101. *Id.* § 2(a)(1).
102. *Id.* § 2(a)(4)-(6).
103. *Id.* § 3(b)(1).
104. *Id.* § 3(b)(2).

utility to consumers" or "that have no significant application for lawful purposes."[105]

The Wyden bill gave examples of TPM limitations that should trigger the disclosure requirement, including limits on users' ability to make time-shifting or space-shifting copies of audio or video content, to make back-up copies to protect against loss, or to use excerpts for such purposes as criticism or commentary, and to transfer one's copy to others.[106] It would have required the FTC to issue an annual report to Congress to review the effectiveness of its notice regulations and to advise Congress about "whether changes in technology or in consumer practices have led to new, legitimate consumer expectations concerning specific uses of digital information or entertainment content that would result in consumers suffering unfair surprise if a technology were to limit those uses without prior notice."[107]

The Wyden bill was explicit about its purposes: to ensure that consumers would have sufficient notice of technical restrictions so that they could "factor this information into their purchasing decisions" and to ensure there was a "strong market-based incentive for the development of technologies that address the problem of unlawful reproduction and distribution of content in ways that still preserve the maximum possible flexibility for consumers to use and manipulate such content for lawful and reasonable purposes."[108]

Even without such legislation, the FTC has authority to regulate unfair and deceptive practices, such as those that may arise from the misuse of TPMs in digital media products. The FTC charged Sony BMG with violating the FTC Act because its copy-protected CDs covertly installed software on purchasers' computers.[109] Sony BMG's failure to give proper notice of the installation of this software was one of the key problems requiring a regulatory response.[110] The FTC's settlement agreement requires Sony BMG to "clearly and prominently disclose" any software that will be installed on user hard-drives or any TPM-based limitations on the usability of the digital content on users' computers. [111]

In a recent address discussing the role of consumer protection in regulating TPMs, FTC Commissioner Thomas Rosch observed that the

---

105. *Id.* § 3(d).

106. Wyden Bill, *supra* note 95, at § 3(c).

107. *Id.* § 3(e).

108. *Id.* § 2(b).

109. Complaint, *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (Jan. 30, 2007), http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf.

110. *See* J. Thomas Rosch, *A Different Perspective on DRM*, 22 BERKELEY TECH. L.J. (forthcoming 2007).

111. Decision and Order of the F.T.C., *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (June 28, 2007), http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf.

Commission "has long insisted that consumers be given adequate notice of the terms on which goods or services are being made available to them, including any material limitations."[112] The FTC had, for example, taken action against the makers of certain wireless devices to require them to inform consumers that purchasing such devices would not provide access to the Internet, and that they had to buy additional products or services to obtain such access.[113] "Likewise, with DRM, *any material limitations of use rights* (including, but not limited to, technological limitations such as an inability to use the media on another platform) *must be clearly and conspicuously disclosed* before a sale of these media is made."[114] This suggests that Sony BMG may only be the first, but by no means the last, deployer of technically protected digital content whose disclosure practices vis-a-vis TPMs will be subjected to regulatory scrutiny by the FTC.

While not expressly calling for regulation to require disclosure of TPMs, a recent report issued by the Center for Democracy and Technology ("CDT") emphasizes the importance of transparency concerning the use of TPMs in mass-marketed digital media products and devices.[115] "With sufficient information, competition between different DRM offerings can help promote a marketplace for digital media products that is diverse and responsive to reasonable consumer expectations."[116] Among the questions the CDT report poses as to transparency are these: "Are users given fair notice of product characteristics that may be relevant to them? Is notice provided in a manner that is sufficiently prominent and understandable? . . . Is notice provided at appropriate times?"[117] "Disclosure is particularly important where DRM-equipped products will not work with certain devices or in certain configurations,"[118] and is "certainly warranted when DRM will

112. Rosch, *supra* note 110, at 3.

113. *Id.* at 3-4 (citing three consent orders in such cases).

114. *Id.* at 4 (emphasis added). In his view, consumers of CDs "have the right to expect that their CDs come without copying limitations, and to expect that the music on those CDs will play on any device." *Id.* at 3. In accordance with this view, Sony BMG could have been charged with unfair and deceptive practices for selling copy-protected CDs without notice, even if it had not also caused rootkit software to be installed on users' computers.

115. *See* CDT REPORT, *supra* note 12, at 2. This report offers four metrics for evaluating DRM products and services: transparency, effect on use, collateral impact, and purpose and consumer benefit. *Id.* at 3.

116. *Id.* at 1.

117. *Id.* at 11. Notice may need to be given not only at the time of the user's first encounter with the product, but also at later times as the user interacts with the product or services related to it. *Id.* at 12. This is especially important if the rights holders offer consumers "upgrades" that, for example, impair compatibility or if the terms of service change in a material way. *Id.* at 13.

118. CDT REPORT, *supra* note 12, at 12. Region-coding restrictions in DVDs, for example, should be disclosed to consumers before they purchase copies that may not work on

cause a product's function to deviate significantly from mainstream consumer expectations. . . ."[119]

The CDT report recognizes that transparency will be thwarted if content producers bury material information about TPM restrictions deep in long license documents that are available to consumers only after they have purchased the product.[120] The report also points to some potential negative impacts of TPMs in digital media products, such as harms to user privacy and anonymity interests insofar as the TPM is programmed to "phone-home" usage information,[121] and harms to competition insofar as TPMs are used to lock users into a particular family of products.[122] CDT urges "[p]roduct reviewers, consumer advocates, and computer security experts [to] be alert for DRM behaviors that pose security risks" such as those caused by the Sony BMG rootkit software.[123]

The notice problem with TPMs, having thus been noticed on both sides of the Atlantic, is ripe for consideration in greater detail regarding the policy options for addressing this problem.

IV. A SPECTRUM OF POLICY OPTIONS TO ADDRESS THE NOTICE PROBLEM

While Part III identified some of the policy options for addressing the problems posed by inadequate or no notice of TPMs that frustrate consumer expectations, we think it is most useful to consider a range of options along a spectrum from least to most regulatory in character, and then to assess the pros and cons of each option.

The least regulatory option is to trust, as we believe copyright industry groups will prefer, that the market can effectively respond to consumer needs for disclosure of TPMs in digital media products. The second, and next lightest, regulatory option would be for the FTC or other consumer protection agencies at the state level to work with copyright industry groups and those concerned about the adequacy of notice as to TPMs to encourage the industry to develop self-regulatory measures to address the TPM notice problem. It is consistent with these first two options for the FTC and similar agencies at the state level to act promptly and decisively when deployers of TPMs deceive consumers or treat them unfairly, as happened in response to the Sony rootkit incident.[124]

---

their machines.

119. *Id.*
120. *Id.*
121. *Id.* at 19.
122. *Id.* at 22.
123. *Id.* at 20.
124. Mulligan & Perzanowski, *supra* note 4.

A third option is for the FTC to undertake a thorough investigation about the uses of TPMs in digital content and the extent to which content owners are disclosing (or not) the capabilities of TPMs that are relevant to consumer decision-making. This investigation would likely produce a report that would recommend whatever legislative or administrative or self-regulatory measures that the investigating agency thought were warranted.

A fourth option would be for Congress to enact legislation akin to the Wyden bill that mandates disclosure of TPMs and gives guidance about some of the functional characteristics (e.g., interoperability across devices) that are of particular legislative concern. As with the Wyden bill, it could leave to the considered judgment of the FTC the decision about what notice should be given in what form as to what products.

A fifth option would not only legislatively mandate that effective notice be given about TPM restrictions or other relevant technical features, but would also substantively regulate certain features in TPM systems, such as privacy-invasive monitoring of consumer usage. In order to give content developers meaningful incentives to comply with notice requirements, Congress might also condition the ability of digital media firms to take advantage of the anti-circumvention rules that protect TPMs used by copyright owners to protect their rights in digital works on their willingness to comply with notice and/or substantive requirements as to TPMs.

Each of these options is discussed below.

A. Trust the Market

Americans generally believe that the market is, or at least can be, an effective means of protecting consumers, especially when there is clear and conspicuous information disclosure and competition among vendors of particular products. If products made by vendor A do not comport with consumer expectations or embody defects likely to harm consumers, vendors B and C will generally be able to lure customers away from A toward their superior or more consumer-friendly products. Comparative advertising, consumer product ratings services, and news media coverage of consumer product issues are among the institutional mechanisms of American markets that contribute to consumer awareness about products and their feature sets. These mechanisms are especially important as to product features that are difficult to discern from pre-purchase visual inspections of the products.

However, consumers of digital media products cannot generally detect TPMs by looking at these products prior to purchasing them; indeed, they may not even learn of the TPMs in the course of ordinary

use of the product.[125] Vendors of digital content have incentives to make the technologies complex, difficult to reverse engineer, and highly proprietary trade secrets in order to inhibit circumventions of the TPMs that would undo the protections they provide.[126] Content owners are also understandably reluctant to disclose TPM restrictions, such as the copy-protection software embedded in some CDs, because consumers do not particularly like TPMs.[127] Consumers who have a choice among digital products, some of which have TPMs and some of which do not, are likely, all other things being equal, to choose the non-TPM'd product.[128] Similarly, consumers are likely to prefer less restrictive TPMs over more restrictive ones, given information relevant to this choice, which helps to explain why Apple's iTunes service has been more successful with consumers than the highly restrictive digital music services offered by major recording industry firms.[129]

The reluctance of vendors to disclose TPM restrictions and features means that members of the public, consumer product reporting services, news reporters, and policymakers are largely ignorant about TPMs. There are, moreover, no established metrics for informing consumers about TPM systems that will affect their usage of digital media products. Although CDT has recently proposed some criteria for metrics to evaluate TPMs,[130] these have yet to take hold as a meaningful market

125. The packaging of DVD movies, for example, does not mention that encryption software installed on the DVD disks prevents backup copying, extraction of fair use snippets, and skipping through commercials. CDT REPORT, *supra* note 12, at 4-5. Consumers are likely to find out about the TPM restrictions only when they try to use the DVD movie in a different way than merely playing it to watch the movie.

126. *See*, *e.g.*, Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 792-95 (2007) (discussing the complex licensing regime that the DVD Copy Control Association has used to maintain secrecy for encryption keys used to protect DVD movies).

127. Disincentives for content developers to disclose TPM restrictions may also arise from concentration in some copyright industry sectors, as in the recording industry. The more concentrated the industry, the less competitive firms may be about key product issues, such as TPMs. Moreover, even in a more deconcentrated industry sector, firms may not want to compete about TPMs because of concerns about fragmentation of the market that might happen during standards wars.

128. Efforts by leading firms in the software industry in the 1980's to use copy-protection technologies were unsuccessful, as TPM restrictions were competed away. *See*, *e.g.*, Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 523-24 (1998).

129. *See*, *e.g.*, Jon Healey, *Bit Player: Sony dis-Connects*, L.A. TIMES, June 18, 2007, http://opinion.latimes.com/bitplayer/2007/06/sony_disconnect.html (discussing the demise of Sony Connect as attributable in part to restrictive TPMs, contrasting this service with Apple's); Yuri Kageyama, *Sony Admits Losing Out on Gadgets; Company Was Hung Up on Content Rights, Executive Says*, WASH. POST, Jan. 21, 2005, at E5 (quoting president of Sony Computer Entertainment admitting that it was overly proprietary in its approach to TPMs and missed out on the unprotected MP3 market).

130. CDT REPORT, *supra* note 12, at 2-3.

constraint on the deployment of TPMs.

While market mechanisms induced some recording industry firms to recalibrate their copy-protection systems to be more consumer-friendly,[131] disclosure of TPM restrictions and capabilities among digital media products remains woefully thin. As Part II has shown, the lack of disclosure has harmed consumers in numerous ways. Given the extent of these harms, we are skeptical that market mechanisms alone will bring about sufficient disclosures about TPMs.[132]

B. Trust Self-Regulation

We are tempted to limit our discussion of the policy option of industry self-regulation to simply stating our belief that self-regulation is unlikely to provide meaningful disclosure about TPM restrictions or capabilities by digital content industry sectors in the absence of significant nudges from governmental actors (on which more in subsection C). However, because this option is often preferred to governmental regulation in the American policy quiver, we will give it somewhat greater attention than it may genuinely deserve.

Self-regulation is often used as an alternative to government regulation in the U.S. This is mainly because firms in an industry are likely to have a more grounded sense about the viability of certain policy options than government regulators. They are in a better position to assess the costs and benefits of various approaches and to identify a range of possible implementations for accomplishing the overall goals. Through self-regulation, firms can apply their expertise to addressing problems in a flexible manner that is responsive to societal expectations.[133] In the course of developing and then implementing "best practices" guidelines or codes of conduct, industry leaders not only internalize the norms that reflect societal values, but also set examples that other firms are likely to follow. Insofar as firms deviate from established self-regulatory norms, there may be both formal and informal means of chastising the deviants and reinforcing the normative heft of the self-regulatory infrastructure.

So why are we skeptical that industry self-regulation is likely to lead to effective disclosure of TPM restrictions and other capabilities

---

131. *Id.* at 7.

132. Our skepticism about the "trust the market" approach was recently reinforced when Sony released another TPM'd product that has reportedly made consumers' computers vulnerable to security attacks. *See* Liam Tung, *Sony Pleads Innocent in Latest Rootkit Fiasco*, ZDNET UK, Aug. 31, 2007, http://news.zdnet.co.uk/security/0,1000000189,39288988,00.htm.

133. *See, e.g.*, Joseph J. Oliver, President & CEO, Inv. Dealers Ass'n of Can., Address at the 85th Investment Dealers Association of Canada Annual Meeting and Conference: The Public Interest in Self-Regulation (June 18, 2001), *available at* http://www.ida.ca/Files/Media/AnnualConf/2001/Speeches/2001OpenAddress_en.pdf.

affecting consumers? For one thing, it has not happened, or even begun to happen, in the past decade. The lack of self-regulatory initiatives is notable, given how common incidents of consumer difficulties with TPMs have been, as shown in Part II. Second, the same disincentives to meaningful disclosure that make us skeptical of a trust-the-market approach undermine our confidence in a self-regulatory approach. Third, a self-regulatory regime is unlikely to succeed because the producers of digital content generally do not construct the TPM systems they use, and each firm has different interests and incentives for paying attention to consumer impacts.[134] Fourth, the most ardent proponents of TPMs, that is, the entertainment industry, has yet to accept that the notice problems identified in this article exist and are in need of attention.[135] This industry does not believe that consumers have "rights" to make backup copies or fair uses of copyrighted content; consumers only have "expectations," and the industry believes that these expectations can be managed by means of the TPMs they build into the digital products and services they make available in the marketplace.

The factor most likely to induce industry self-regulation of TPMs in the U.S. is the adoption of disclosure requirements for TPMs by other nations, such as the U.K. Because markets for digital media products are global, disclosure regulations in even one country with a sizeable market may well affect industry behavior worldwide. However, it is also quite possible that the industry will choose to segment the market by selling products with notices in places that require them and products without notice where transparency is not required.

C. An FTC Investigation and Report

By bringing a claim against Sony BMG in response to the rootkit software incident, the FTC has demonstrated that it already has authority to regulate abusive uses of TPMs in mass-market products. Lack of meaningful disclosure was a key element of this case, and to settle this lawsuit, Sony BMG pledged to disclose material features of TPM systems in audio CDs in the future.[136]

The broader implications of the *Sony BMG* case, however, are

---

134. *See, e.g.*, Mulligan & Perzanowski, *supra* note 4.

135. *See, e.g.*, Preston Padden, Executive Vice President, Walt Disney Co., Remarks at the Silicon Flatirons Conference: Digital Rights Management (Feb. 11, 2007) (endorsing a trust-the-market approach). The videogame industry also widely uses TPMs without giving notice about TPM restrictions; they have yet to feel any public pressure to provide meaningful notice of TPMs.

136. Decision and Order of the F.T.C. at 3-5, *In re* Sony BMG Music Entm't, File No. 062-3019, Dkt. No. C-4195 (June 28, 2007), http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf (setting forth consent decree disclosure requirements).

apparent from Commissioner Rosch's affirmation that failure to reveal relevant technical restrictions to consumers prior to their purchase of technically protected digital media products may be an unfair or deceptive trade practice.[137] As we have shown, Sony BMG is far from the only deployer of TPMs that has given little or no information to consumers about the restrictiveness of their systems.

While the FTC will almost certainly bring additional cases against firms that abusively deploy TPMs in digital products, we believe that the Commission should launch an investigation into the extent of transparency about TPMs in mass-marketed software and digital media products (or lack thereof) and consumer harms resulting therefrom, and issue a report akin to those it has written on other new technology consumer protection issues, such as spyware and online information privacy.[138] Part II cites many examples of transparency problems with TPM deployments, which suggests that a broad empirical investigation is warranted of industry practices as well as the mismatch between consumer expectations and TPM restrictions and features. Such a report might recommend legislation or other measures aimed at bringing about greater transparency about TPMs.

It is even conceivable that such a report, or perhaps even the prospect of such a report, will induce those who are regularly deploying TPMs in digital products to commence a conversation about self-regulatory measures that might be undertaken to address the notice problems we have identified here. While we have doubts about how meaningful any such effort would be without the prospect of closer regulatory oversight hanging like a sword of Damocles over their heads, it would be a welcome development for the affected industry groups to begin to address the notice problem in a constructive way.

D. Conditioning Legal Protection for DRM on Adequate and Effective Notice

Designing the proper regime for enforcing adequate and effective DRM notice depends on many factors, incentives, and efficiencies. One approach to balancing these factors is delegation to an experienced federal agency such as the FTC, as detailed in Section C above. An alternative approach, however, would be to focus less on government regulation via central agency and more on market incentives tied to legal

137. Rosch, *supra* note 110, at 4.

138. *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; FED. TRADE COMM'N, MONITORING SOFTWARE ON YOUR PC: SPYWARE, ADWARE, AND OTHER SOFTWARE (2005), *available at* http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

entitlements.

Section 1201 of the Digital Millenium Copyright Act[139] provides a strong legal incentive for firms to incorporate TPMs into their products and provides strong intellectual property right-like protection against the circumvention of TPM systems. However, unlike most other intellectual property grants,[140] it does not provide sufficient incentives to give notice of the scope of the associated rights and restrictions it protects. One option for encouraging firms to take on the obligation to provide meaningful notice in a serious way would be to condition standing to sue under Section 1201 on the requirement that the party intending to sue "provide reasonable and effective notice of all access and/or copy limitations implemented by the technical measure protected under this title." This would ensure that those firms, especially those in the entertainment industry, who rely heavily on Section 1201, take the steps necessary to explicitly describe the contours and limitations they wish to protect from circumventing acts and devices.

A second additional incentive would be to require knowledge and/or intent for violations of Section 1201. Other systems of intellectual property rights have mechanisms for giving adequate and effective notice of the metes and bounds of one's property right, which are often important triggers to "intentional" or "willful" liability for infringement of the right.[141] As noted above in Part II, adequate and effective notice was and should be one of the key concerns raised in cases such as *Lexmark* and *Skylink*. Recall that the defendants in those cases did not have adequate notice that copyrighted works were even allegedly protected by a 1201-relevant TPM, let alone actually protected by one. Thus, even if there had been a violation of Section 1201 in those instances, it would have almost certainly been an unintentional one.

By requiring that the plaintiff in a Section 1201 case prove that the defendant knew it was circumventing or intended to circumvent the known restrictions on access or copying, potential plaintiffs would have

---

139. 17 U.S.C. § 1201.

140. *See, e.g.*, 17 U.S.C. §§ 411(a), 412 (requiring registration of copyrighted materials prior to institution of suit and as prerequisites for statutory damages and attorneys fees and costs); 35 U.S.C. § 287(a) (2000) (denying recovery for patent infringement damages prior to the issuance and recording of a patent in the Federal Register unless the patentee has given notice to the public by marking); 15 U.S.C. § 1111 (2000) (denying profits and damages for trademark infringement without proper notice of registration); CAL. CIV. CODE § 3426.1(b) (West 2007) (requiring actual or constructive knowledge of trade secrecy or improper acquisition in order to find liability for misappropriation).

141. *See, e.g.*, 17 U.S.C. § 504(c)(2) (raising ceiling on statutory damages for willful copyright infringement from $30,000 per work to $150,000 per work); CAL. CIV. CODE § 3426.3(c) (West 2007) (authorizing exemplary damages up to twice actual damages for willful or malicious trade secret misappropriation); 35 U.S.C. § 284 (authorizing treble damages for willful patent infringement).

incentives to give clear, adequate, and effective notice of TPM restrictions in order to make their case as easy as possible to win. Without proper notice, defendants should be able to legitimately defend against Section 1201 charges if they had no knowledge of the TPM or intent to circumvent it.

A change of this sort could be implemented in at least two ways. First, courts could decide that defendants who could not have anticipated potential 1201 liability for developing technologies or reverse engineering TPMs should not be deemed to violate 1201 on fundamental fairness grounds. Second, Congress could insert the word "knowingly" before the word "circumvent" in Section 1201(a)(1)(A). For the trafficking provisions of 1201(a)(2) and (b)(1), one would insert "knowingly" before the word "manufacture". This would ensure that in order for a defendant to be found liable under Section 1201, it must know of the existence of the access or copy control and know that either it is circumventing that TPM or that the primary purpose of the device it is trafficking in is to do so. This would negate liability for those innocently caught in the web of undisclosed TPMs like the defendants in the *Lexmark* and *Skylink* cases, while still holding liable those who intentionally circumvent TPMs or assist other in circumventing TPMs to facilitate infringing acts. These are the bad actors that Section 1201 was truly intended to reach.

Conditioning the ability to bring 1201 claims on giving consumers adequate and effective notice of TPM restrictions is consistent with the WIPO Copyright Treaty, the international agreement which first called for regulation of circumvention of TPMs.[142] Under that treaty, nations are required to adopt anti-circumvention regulations to punish those who defeat TPMs in order to facilitate copyright infringements. However, the treaty was also intended to limit the scope of these technological and legal tools from impeding legitimate acts that were permitted by law or otherwise beyond the authority of copyright owners, such as fair use of copyrighted works or unfettered access to public domain works.[143] Adding notice of TPM requirements and/or knowledge and intent requirements to Section 1201 supports this goal, as it would encourage TPM vendors and copyright owners to make sure their technological restrictions are in line with the limits of their rights; failure to do so

142. *See* World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65, *available at* http://www.wipo.int/clea/docs_new/pdf/en/wo/wo033en.pdf.

143. *See, e.g.*, *id.* at Art. 11 (requiring the parties to legally protect and enforce TPMs, but only to the extent that the TPM operates against unauthorized or illegal uses). For a discussion of the balance embedded in this provision, see, *e.g.*, J.H. Reichman, Graeme Dinwoodie & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Works*, 22 BERKELEY TECH. L.J. 981 (2007).

would not only risk critical public scrutiny but also forfeiture of Section 1201 enforceability.[144]

E. Substantive Consumer Protection Laws

A final policy response to consumer protection concerns posed by TPMs would be to consider enacting new laws that would substantively address specific harms identified in Part II above, perhaps even a "digital consumer bill of rights." For example, Congress could outlaw the use of TPMs that substantially impair the use of computers and digital content in ways unrelated to the lawful exercise of copyright owner control over access to or copying of copyrighted works protected by TPMs or use of TPMs that increased the risk of unauthorized access by third parties.[145] Congress could also outlaw any TPM that collects non-public data on consumer uses of technically protected content without independent and explicit consent by each computer user and for each new use of that data. An alternative would be to allow collection and transmission of data but condition these activities on anonymizing the data so that it could not be linked back to any particular user or individual.[146] Finally, Congress could pass laws enabling users to circumvent TPMs for public interest uses.[147]

CONCLUSION

There are many reasons why it is socially desirable for producers of digital content to give effective notice about TPMs embedded therein. Such notice is obviously likely to affect decisions about whether to purchase technically protected products and may induce shopping for alternatives. Notice will also affect consumers' assessment of the value they will derive from purchasing such products and their satisfaction

144. A conditional requirement is already present in 17 U.S.C. § 1201(k)(2), which requires those who use copy-control technologies for videocassette recorders to maintain consumer capabilities to engage in time-shifting of broadcast and some cable television content. Other scholars have similarly suggested conditioning section 1201 enforcement on copyright owner willingness to respect legitimate consumer concerns, such as the right to gain access to TPM content for fair use purposes. *See generally*, Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41, 55-58 (2001).

145. This would be consistent with the European Union's implementation of the WIPO Copyright Treaty which imposes an obligation on EU member states to ensure that consumers will be able to exercise exceptions and limitations even when works are technically protected. *See* Reichman, Dinwoodie & Samuelson, *supra* note 143, at Pt. III.

146. *See, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) (discussing the value of intellectual privacy, and legal bases for protecting it from infringing TPMs).

147. *See* Boucher Bill, *supra* note 88; Reichman, Dinwoodie & Samuelson, *supra* note 143.

with them. Notice of TPMs can, moreover, avert imposing unwarranted burdens on retailers, consumer electronics firms, and makers of digital media players whom frustrated consumers may otherwise blame for upsetting experiences with TPMs of which they had no notice.[148] Product reviews by consumer rating services and the news media will also be better able to inform consumers if producers of digital content with TPMs reveal more about product characteristics and limitations.[149]

Requiring firms to give consumers notice about TPMs is more likely to foster meaningful competition among providers of digital products and services than will occur if giving notice about TPMs is not required. Some of this competition will be between TPM and non-TPM products, and some will be between products with more and less restrictive TPMs.[150] Even in the absence of competition, digital media producers may be affected by notice requirements when making decisions about whether to use TPMs or whether to use lighter- or heavier-weight TPM systems. The more notice they have to give about the restrictiveness of their products, the less inclined they may be to adopt highly restrictive systems.

We are not so naïve as to believe that designing effective disclosure rules about TPMs will be easy. The products and services to which notice requirements may apply are so varied, as are the devices on which the content can be rendered and the capabilities of TPM systems. Fortunately, the FTC has demonstrated considerable competence in balancing consumer and producer interests in other new technology contexts, and we, like Rep. Boucher and Senators Brownback and Wyden, are confident that the Commission can devise a flexible and adaptable disclosure regime that will yield notices that consumers can understand and that copyright owners can live with.

Nor are we naïve as to believe that a notice requirement will address all of the consumer protection issues likely to be posed by TPMs in digital content. Although consumer protection laws, such as those administered by the FTC, have proven flexible enough to deal with the first round of TPM consumer protection problems, we foresee the

148. *See* Digital Media Consumers' Rights Act of 2005, H.R. 1201, 109th Cong. § 2(1).

149. *See generally* CDT REPORT, *supra* note 12.

150. That competition is having an effect on the use of TPMs is evident from the recent decision of one of the major recording labels, EMI, to allow much of its repertoire to be distributed via digital music services in an unprotected MP3 format, instead of being locked down with TPMs. *See, e.g.*, Press Release, EMI Group Ltd., EMI Music Launches DRM-Free Superior Sound Quality Downloads Across Its Entire Digital Repertoire (Apr. 2, 2007), *available at* http://www.emigroup.com/Press/2007/press18.htm. Even though the Apple iTunes service currently uses TPMs, Steve Jobs, Apple's CEO, has announced its willingness to drop TPM restrictions on digital music and has urged major labels to agree to this. *See, e.g.*, Posting of Steve Jobs on Apple Inc., Thoughts on Music, http://www.apple.com/hotnews/thoughtsonmusic/ (Feb. 6, 2007).

possibility of the need for additional regulation of TPMs over time. Especially likely to be needed is regulation to protect information privacy of users of TPM'd content insofar as the TPMs are part of a monitoring regime affecting consumer intellectual privacy interests.

TEMPTATIONS OF THE WALLED GARDEN: DIGITAL RIGHTS MANAGEMENT AND MOBILE PHONE CARRIERS

NEIL WEINSTOCK NETANEL*

Content industries have long heralded Digital Rights Management ("DRM"), the use of technological protection to control and meter access to digital content. They view DRM as the key to securing copyrighted expression against massive digital piracy and thus to enabling the industries to distribute their movies, sound recordings, and books in the digital network environment.

Receptive to the content industry call, Congress prohibited the circumvention of such technological protection measures when it enacted the Digital Millennium Copyright Act of 1998 ("DMCA").[1] It did so with the express purpose of furthering copyright law's goal of promoting the creation and dissemination of original expression. As the Senate Report accompanying the Act announced, by creating "the legal platform for launching the global digital online marketplace for copyrighted works," the anti-circumvention provisions sought to "make available via the Internet the movies, music, software, and literary works that are the fruit of American creative genius."[2]

Yet, ironically, DRM is often used to lock in consumers to ancillary products and services in ways that might hamper markets for distributing cultural expression. Apple's iTunes is the most widely publicized example. Apple's combined ACC file format and Fair Play DRM render music and video downloaded from iTunes unplayable on portable media players other than Apple's iPod.[3] Likewise, Apple's iPod will not play

* Professor, UCLA School of Law. My thanks to the organizers and participants in the Digital Broadband Migration Conference, February 11-12, 2007, at which I presented an earlier version of this essay. I also thank Talal Shamoon and Soichiro Saida for graciously sharing their insights about DRM and mobile carriers, and my research assistants, Lisa Kohn and Wyatt Sloan-Tribe, for their excellent work. All errors are mine.

1. The DMCA provisions are actually both narrower and broader than the summary statement in the text suggests. They are narrower because they do not universally proscribe circumvention of the DRM. They are broader because, in addition to prohibiting circumvention, they prohibit trafficking in devices whose primary design is to enable DRM circumvention. *See infra* notes 26-28 and accompanying text.

2. S. REP. No. 105-190, at 2 (1998).

3. Consumers with the knowledge and time to do so can evade these limitations by burning iTunes music onto a CD in MP3 format and then transferring it to another player. But

proprietary formatted music or video downloaded from online content distribution sites that compete with iTunes (but will play generic MP3s). Apple uses DRM not just to limit unlicensed copying of content, but to anchor its dominance in the market for portable media players and online music distribution. Much to the consternation of the music industry, this puts Apple in the driver's seat in bargaining for licensing terms for music distribution on iTunes.[4] And Apple's DRM-driven defeat of interoperability is blamed by some consumers and technology companies (primarily Apple's rivals) for stifling the growth of the legal digital music download market.[5]

Apple insists that its DRM restrictions have been forced upon it by the record labels and indeed that Apple must maintain a closed proprietary system in order to meet its contractual commitments to the labels to expeditiously remedy any compromise of DRM controls.[6] In that vein, Apple has called upon the recording industry to "abolish DRMs entirely" and has contracted with EMI to distribute a portion of that major label's catalogue free of DRM.[7] However reluctantly, other labels might follow suit.[8]

Commentators sharply disagree on whether Apple truly desires to sell DRM-free music or aims simply to placate consumer advocates and regulatory authorities who have been pressing the company to make the iPod/iTunes system interoperable with other technology platforms.[9] With Apple's June 2007 release of its much touted iPhone, that debate, as well as the debate over interoperability in general, has expanded to the

---

for most users, the Apple limitations are sufficiently burdensome to curtail interoperability.

4. *See* Yinka Adegoke, *Apple Seen Having Upper Hand in Music Negotiations*, REUTERS, Apr. 20, 2007, http://www.reuters.com/article/technology-media-telco-SP/idUSN1832165720070423 (noting that the labels are beholden to Apple, which has more than 80 percent of all digital music download sales in the United States).

5. For more on the FairPlay controversy, *see* Nicola F. Sharpe & Olufunmilayo B. Arewa, *Is Apple Playing Fair? Navigating the iPod FairPlay DRM Controversy*, 5 NW. J. TECH. & INTELL. PROP. 332 (2007). *See also* Christopher Sprigman, *The 99¢ Question*, 5 J. ON TELECOMM. & HIGH TECH. L. 87, 111-12 (2006) (discussing AAC file format and FairPlay DRM restrictions on interoperability).

6. Steve Jobs states that repairing a leak would be "near impossible if multiple companies control separate pieces of the puzzle, and all of them must quickly act in concert." Apple Inc., Thoughts on Music, http://www.apple.com/hotnews/thoughtsonmusic (last visited Sept. 26, 2007).

7. *See id*.; s*ee also* Brian Garrity, *Adding Up iTunes Plus*, BILLBOARD MAG., June 23, 2007, at 7 (reporting on sales data for DRM-free EMI music on iTunes).

8. *See* Adegoke, *supra* note 4.

9. *Id*. (reporting the view of "cynical observers" that Apple's call to drop DRM "was sparked by pressure . . . from European regulators to open the iPod/iTunes family to other technology platforms); *see also* Ethan Smith & Nick Wingfield, *EMI to Sell Music Without Anticopying Software*, WALL ST. J., Apr. 2, 2007, at B5 (reporting on EMI move, Apple's call to drop DRM, and pressure on Apple by consumer-rights organizations and regulators in several European countries).

mobile carrier arena. Whether due to Apple's contractual obligations or underlying self-interest, Apple and its iPhone partner, AT&T Wireless, have extended and deepened the ACC/FairPlay DRM model. The iPhone and AT&T Wireless subscription agreement follow a proprietary, "walled garden" approach. The iPhone and any iTunes music residing on it may be used and accessed only by AT&T subscribers.[10] And the iPhone may not be used to play proprietary formatted music of iTunes competitors or place phone calls through networks other than AT&T's.[11]

The iPhone is a combined iPod, smartphone, and Internet search device.[12] Each function is hardwired to secure the Apple-AT&T walled garden. In its iPod capacity, the iPhone adopts much the same walled garden functionality as the iPod, with additional restrictions tied to the AT&T subscription. Like the iPod, the iPhone is designed to import music only through the iTunes program on the user's computer and will not play music in rival distributors' proprietary formats. In addition, the iPhone is hardwired to work only if activated by acquiring a two-year cellular subscription with AT&T Wireless, which users initiate when they first connect the iPhone to the iTunes software on their computer.[13] And if the AT&T subscription lapses, the iPhone will no longer work – not as a phone, not as a music and video player, and not as an Internet

10. The iPhone is bundled with a two-year subscriber contract with AT&T Wireless, which will be the exclusive carrier of the iPhone at least until 2009. *See* AT&T Wireless, iPhone Exclusively From AT&T and Apple, http://www.wireless.att.com/cell-phone-service/specials/iPhoneCenter.html (last visited Sept. 26, 2007).

11. The applicable AT&T Terms of Service provide: "Equipment purchased for use on AT&T's system is designed for use exclusively on AT&T's system. You agree that you will not make any modifications to the Equipment or programming to enable the Equipment to operate on any other system." Apple Inc., AT&T – Terms of Service, http://www.apple.com/legal/iphone/us/terms/service_att.html (last visited Oct. 17, 2007). In tandem, Apple's iTunes Terms of Service provide that "[u]se of the Service requires a compatible device" and that "Apple and its licensors reserve the right to change, suspend, remove, or disable access to any Products, content, or other materials comprising a part of the Service at any time without notice." Apple Inc., Apple and Third Party Terms and Conditions, http://www.apple.com/legal/iphone/us/terms/service_all.html (last visited Oct. 17, 2007).

12. For thorough reviews of iPhone features and restrictions, *see* Walter S. Mossberg & Katherine Boehret, *Testing Out the iPhone*, WALL ST. J., June 27, 2007, at D1; Kent German & Donald Bell, Review, *Apple iPhone - 4GB (AT&T)*, C/NET, June 30, 2007, http://reviews.cnet.com/4505-6452_7-32180293.html.

13. Almost immediately after the iPhone's release, hackers discovered ways to activate the iPhone's web browser and iPod without signing an AT&T contract. But few users will have the technical know-up, or incentive (having spend upwards of $500 for an iPhone), to do so. *See* Li Yuan, *Hackers Bypass iPhone Limits*, WALL ST. J., July 6, 2007, at B4. Moreover, Apple responded to the hackers by releasing an iPhone software update that turns unlocked iPhones into functionless "bricks." *See* Katie Hafner, *Altered iPhones Freeze Up*, N.Y. TIMES, Sept. 29, 2007, at C1. For its part, AT&T has threatened legal action against anyone who offers instruction or tools to unlock the iPhone. *See* Jennifer Granick, Commentary, *Legal or Not, iPhone Hacks Might Spur Revolution*, WIRED, Aug. 28, 2007, http://www.wired.com/politics/onlinerights/commentary/circuitcourt/2007/08/circuitcourt_0829.

search device. At the same time, just as Apple's combined ACC file format and Fair Play DRM renders iTunes content unplayable on rival portable media players, the iPhone and possibly other AT&T handsets, such as the Motorola RAZR V3i, will be the only mobile carrier handsets capable of transferring and housing iTunes music and video from the user's personal computer. The iPhone will sport Wi-Fi and Internet browsing capability. But it will not support downloading Voice-over-IP clients such as Skype, so it will be capable of making and receiving telephone calls only through the AT&T cellular network.

The Apple-AT&T walled garden approach, in short, employs a combination of DRM and proprietary format to attract and then lock in consumers to the iPhone and AT&T subscription. Consider a consumer who purchases an iPhone and signs up for a two-year AT&T contract. At the very least, the consumer is locked in to the AT&T service for the two years of the contract.[14] That is already common practice for mobile telephone service. What Apple adds is an additional layer of stickiness at the end of the contract. The consumer who moves to another carrier will no longer be able to use her iPhone. She will not only require her new carrier's handset to engage in cellular communications; she will also lose the ability to use the iPhone as an Internet search device and media player. If she wants to continue to play her iTunes content on a mobile device, she will have to purchase an iPod.[15]

While the iPhone and iTunes will be available exclusively for AT&T subscribers, AT&T provides music, video, and games from other sources for use on other handsets as well. AT&T is not alone. Mobile carriers are rapidly becoming multimedia data portals and distributors. In most countries, markets for basic cellphone service are becoming saturated. As a result, wireless carriers and handset manufacturers are racing to develop technologies and business models for some combination of streaming and downloads of videos, live TV programming, music, web browsing, multiplayer gaming, social networking, and information, such as GPS, local traffic reports, and weather conditions, tailored to people on the go.[16] Like the iPhone, in

14. AT&T's Terms of Service provide that a customer who terminates the service prior to expiration of the two-year period must pay a termination fee in the amount of $175 for each wireless telephone number associated with the service. AT&T – Terms of Service, *supra* note 11.

15. XM satellite radio follows a similar model for its mobile player device, the Inno; songs recorded from XM radio onto the Inno can no longer be accessed if the XM radio subscription lapses (or indeed if the Inno fails to receive at least 8 hours of live XM radio signal per month in order to authenticate the user's subscription). *See* PIONEER ELECS. SERV., INC., INNO USER GUIDE 26 (2006), *available at* http://www.xmradio.com/pdf/hardware_support/pioneer/inno/userguide.pdf.

16. J.A. Harmer, *Mobile Multimedia Services*, BT TECH. J., July 2003, at 169; Li Yuan, *Cellphone Video Gets on the Beam*, WALL ST. J., Jan. 4, 2004, at B3.

short, cell phones are metamorphosizing into multi-purpose, multi-media communications, information, content player, and content receiver devices. Industry analysts predict that mobile content and entertainment revenues will grow exponentially in Europe and the United States over the next several years, with U.S. revenues reaching $50 billion by 2010.[17]

The Apple-AT&T walled garden approach to locking in consumers (or at least erecting barriers to consumer mobility) might be attractive for other mobile carriers as well.[18] Mobile communications carriers have long sought to combat customer churn. They have used a variety of devices to do so, including long-term subscriber contracts, deploying DRM to lock handsets so the handset cannot be used with a different carrier, and requiring consumers to change their telephone number when moving to a new carrier. Churn rates have declined over the past year or two, whether because of the success of these tools (other than that of requiring consumers to change their telephone numbers, since the FCC now requires number portability), greater consumer satisfaction with existing carriers, or industry consolidation and its resulting reduction in competition.[19] Nevertheless, churn rates remain high, reportedly resulting in a loss of between 18 and 36 percent of subscribers each year.[20] Applying DRM to condition subscribers' access to music, video, and other content upon their continued use of the carrier's service presents yet another tool for combating subscriber churn.

To a certain degree, the leading carriers already use DRM to tether content to their service. When subscribers move to a new carrier they typically lose any ringtones, video, music, or games they downloaded onto their handset because their handset cannot be used with the new carrier. The carriers do sometimes enable subscribers to move downloaded content from their handset to their computers in a standard format. The Verizon V-Cast and Sprint Digital Lounge music services, for example, allow subscribers to transfer downloaded music from their handsets to their computers in Windows Media format. Handsets can

---

17. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIGITAL BROADBAND CONTENT: MOBILE CONTENT - NEW CONTENT FOR NEW PLATFORMS 9 (2005), http://www.oecd.org/dataoecd/19/7/34884388.pdf.

18. *Cf.* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 109-10 (1998) (discussing strategies to deter customer mobility by imposing switching costs); *see also* Robert Cyran & Edward Hadas, *Learning From Palm's Pain*, WALL ST. J., Mar. 6, 2007, at C2 (contending that consumer technology firms in general would do better to build "sticky features" into their products to give consumers a disincentive to switch to rival devices).

19. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, *Report*, 21 Fcc Rcd. 10,947, 11,011-13 (2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-142A1.pdf [hereinafter FCC 2006 Mobile Services Report].

20. *Id.*

also be designed to store content obtained from third parties, much like MP3 players. In these instances, the use of DRM to render handsets incompatible with other carriers is more a hindrance than a significant barrier to moving to a new mobile carrier. While a subscriber who leaves Verizon or Sprint must typically obtain a new handset for his new carrier, he can still transfer music from his computer to his new handset, so long as it is Windows Media compatible.

Mobile carriers, in short, have a variety of technological and market options for using DRM to erect a walled garden and tether content to their services as a means of locking in consumers. (I realize that "lock-in" is overstating. I mean it as a shorthand for creating greater stickiness, imposing a cost on consumer mobility, not an absolute barrier.). The use of DRM to combat mobile subscriber churn is quite different, and may have different regulatory implications, from DRM's use to protect content against copyright infringement. This paper entertains the possibility that mobile carriers will follow the Apple-AT&T walled garden approach. It considers the regulatory implications of mobile carriers' design and use of DRM to lock in their subscribers as opposed to deploying DRM to protect rights in the content itself by preventing the music and video that subscribers purchase from leaking out into unlicensed peer-to-peer file trading networks. AT&T has already threatened legal action against those who offer instructions or tools to unlock the iPhone.[21] How does and should the law view the Apple-AT&T use of DRM to enforce their iTunes/iPhone/AT&T network walled garden and others' efforts to break down the walls by hacking the iPhone and FairPlay DRM?

I first consider whether consumers would and should be able to circumvent such DRM under the DMCA. Does a mobile carrier's use of DRM to lock in consumers to its service serve the goals of the DMCA? In answering that question, should it matter whether the carrier deploys DRM on copyrighted content as opposed to using DRM simply to lock the handset? And under judicial interpretation of the DMCA, would circumvention for the limited purpose of being able to move to a new carrier and still access content the consumer purchased from his prior carrier violate the anti-circumvention proscriptions of the Act? I then consider mobile carriers' use of DRM to lock in consumers from the telecommunications regulation perspective. The FCC mandated number portability, but refused to ban handset locks. How might it regard and how should it regard content mobility under current market conditions?[22]

---

21. For discussion of AT&T's threatened legal action, *see* Granick, *supra* note 13.

22. I do not consider a possibly relevant third legal regime: claims by consumers against mobile phone manufacturers or carriers who deploy DRM to disable a handset or service in response to the consumer's unlocking of the handset. A class action lawsuit recently filed

Before I proceed, I want to clarify: it is by no means a foregone conclusion that mobile carriers will follow the walled garden approach rather than one that allows for interoperability. Markets for digital distribution of content are in great flux and mobile carriers stand at a crossroads regarding their business model for multimedia content distribution, choice and application of DRM, and selection of strategic partners. On one hand, using DRM to establish a proprietary, branded content distribution network, and to lock in subscribers at the same time, offers the potential to capture substantial rents. Apple has done very well with its iTunes/iPod model by creating a high quality, user friendly, attractively branded end-to-end experience. But on the other hand, consumers want interoperability. They want to be able to seamlessly transport content and applications from one device and service to another. Apple's proprietary model for computers did not fare so well against the greater interoperability of the Windows/PC platform.

Industries typically seek some element of proprietary product and branding. No firm wants to compete in a fully commodified market if that can be avoided. In these early days of entering the multimedia content distribution market, mobile carriers have yet to determine the extent to which deploying DRM to help secure their proprietary networks is a viable long-range option.

The Open Mobile Alliance's DRM standard reflects that ambivalence. The Open Mobile Alliance is a telecommunications, information technology, and content industry umbrella organization, with the stated mission "to facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, while allowing businesses to compete through innovation and differentiation."[23] The Alliance, which counts the leading mobile carriers (as well as handset manufacturers and IT companies) among its members and sponsors, has released a DRM specification called OMA 2.0 for use in mobile handsets and other consumer electronics devices.[24] OMA 2.0 is designed to enable content providers,

---

against Apple alleges that Apple's extrajudicial enforcement of the iPhone-AT&T Wireless bundle through iPhone software updates that render unlocked iPhones into functionless "bricks" violates California antitrust and unfair competition law. *See* Complaint for Treble Damages and Permanent Injunctive Relief, Smith v. Apple Inc., No. 1-07-CV-095781 (Cal. Super. Ct. Oct. 5, 2007), *available at* http://www.appleiphonelawsuit.com/uploads/Class_Action_Complaint__Smith_vs_Apple.pdf.

23. Open Mobile Alliance, http://www.openmobilealliance.org/ (last visited Sept. 27, 2007).

24. *See* Open Mobile Alliance, OMA Release Program and Specifications, http://www.openmobilealliance.org/release_program/drm_v2_0.html (last visited Sept. 27, 2007).

mobile carriers, and others to wrap content to enable consumers to transport content across several registered devices. But it also enables a provider or mobile carrier to place obstacles to interoperability and transportability.[25]

I. DIGITAL MILLENNIUM COPYRIGHT ACT

With the advent of digital technology and the Internet, copyright industries faced the threat of massive unlicensed copying and distribution of their copyrighted works. In response, the industries began to deploy technological protection measures, including digital encryption, to control access to and copying of their content. Enacted in 1998, the Digital Millennium Copyright Act ("DMCA") neither mandates nor restricts the use of such technological protection measures (which have come to be called Digital Rights Management ("DRM"), inaccurately because they can be used to secure content and services beyond the scope of any preexisting legal "rights"). Rather, the DMCA contains far-reaching provisions designed to combat the circumvention of those technological protection measures that are deployed to control access to or uses of copyrighted content.

The DMCA's anti-circumvention provisions are of two basic types. First, the DMCA prohibits users from circumventing technology that controls access to protected works.[26] Second, the Act prohibits the manufacture and trafficking of devices, technology, and services that are primarily designed to assist users in circumventing technology that (1) controls access to content that is protected under the Copyright Act,[27] or (2) effectively protects a copyright holder right by controlling uses of such content.[28]

---

25. It is sometimes said that DRM, by its very nature, must impose some limits on interoperability and transportability. As one knowledgeable observer states:

> '[T]ruly interoperable DRM' . . . is a fallacy. By definition, there is no such thing, nor can there be. The whole point of DRM is being able to control the use and distribution of content. . . . If the DRM restrictions were too liberal, then the music files could be easily shared. That would obviously defeat the purpose of using DRM in the first place.

Technical Conclusions, http://technicalconclusions.wordpress.com/2007/02/22/thoughts-on-drm-part2/ (Feb. 22, 2007) (blog posting titled Thoughts on DRM: Part II). The idea that DRM means limits on interoperability may well be true for DRM that aims to control the use and distribution of content. But it does not hold for DRM that aims only to meter uses on any device on which the content is used, for purposes of extracting payment from the user or a third party, such as the device or service provider or an advertiser. *See* Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003) (presenting a blueprint for using DRM to meter, but not control, personal, noncommercial uses of digital content).

26. 17 U.S.C. § 1201(a)(1)(A) (2000).

27. *See id.* § 1201(a)(1)(E).

28. *See id.* § 1201(b).

As the Second Circuit has put it, in outlawing the circumvention of access controls and prohibiting circumvention devices, "Congress sought to combat copyright piracy in its earlier stages, before the work was even copied."[29] Others have posited that even though copyright law does not accord copyright owners with an exclusive right to control access to their works, the DMCA's access prohibition provides the legal framework for copyright holders to market various forms of access, ranging from streaming to pay-per-use, as an alternative to selling permanent copies.[30] In that way, copyright industries will be able to charge differential prices tailored to consumer demand, and consumers will correspondingly have the option of buying access to content on a subscription model or paying for a one-time viewing or listening rather than purchasing a permanent download.

At the same time that it provided legal support for a pay-per-use business model, Congress expressed concern that pay-for-use might run amok, that it might ultimately reduce, rather than enhance, access to "copyrighted materials that are important to education, scholarship, and other socially vital endeavors."[31] Congress particularly feared the "perfect storm" combination of the elimination of print or other hard-copy versions, permanent encryption of all electronic copies, and adoption of business models that restrict distribution and availability of works.[32] To address that concern and "maintain balance between the interests of content creators and information users," Congress delegated to the Librarian of Congress the power to suspend application of the access prohibition to the extent and duration required to prevent "a diminution in the availability to individual users of a particular category of copyrighted materials," particularly for favored, productive uses such as scholarship, education, criticism, and news reporting.[33] The Act provides for a Library of Congress rulemaking every three years so that the Librarian can determine, upon the recommendation of the Register of Copyrights (who must consult with the Assistant Secretary for Communications and Information of the Department of Commerce), whether the prohibition adversely impacts persons' "ability to make non-infringing uses under this title of a particular class of copyrighted works."[34] If the Librarian finds such adverse impact, the prohibition does not apply to "such users with respect to such class of works for the

29. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 2001).

30. *See* Jane Ginsburg, *From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law*, 50 J. COPYRIGHT SOC'Y 113 (2003).

31. H.R. REP. No. 105-551, pt. 2, at 36 (1998).

32. *Id.*

33. *Id.* at 35-36; 17 U.S.C. § 1201(a)(1)(C).

34. 17 U.S.C. § 1201(a)(1)(C).

ensuing 3-year period."[35]

The Library of Congress rulemaking and case law applying the DMCA both impact the extent to which mobile subscribers may lawfully circumvent mobile carriers' DRM. I consider each in turn.

A. Library of Congress Rulemaking

In his November 2006 rulemaking, the Librarian exempted from the access prohibition "[c]omputer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."[36] In promulgating the three-year, possibly renewable exemption, the Librarian found that the handset "access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to switch to other carriers, a business decision that has nothing whatsoever to do with the interests protected by copyright."[37] As of November 2006, therefore, consumers and others may unlock a handset in order to enable its use for wireless communication through a new mobile carrier.

It is easy to see why carriers lock handsets to reduce subscriber churn. A locked handset imposes an immediate cost on a subscriber who wishes to switch carriers: the subscriber must buy a new handset and spend the time to personalize it by entering contact lists and the like. In addition, the subscriber loses any content – music, videos, and photographs – that are stored on the locked handset. At a minimum, the subscriber must retrieve and transfer copies of that content from the subscriber's PC to her new handset. And depending on circumstances and any DRM limitations imposed on the content itself, the subscriber might simply lose the sunk cost of purchasing it through her previous carrier.

The Library of Congress rule might appear to greatly undermine mobile carrier efforts to combat churn through locking handsets. Most obviously, the exemption makes it possible for subscribers to save the costs of purchasing a new handset and re-inputing personal information. In addition, if subscribers can take their old handsets with them, they might also be able to continue to access whatever downloaded content

35. *Id.* § 1201(a)(1)(D).

36. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,476 (Nov. 27, 2006) (to be codified at 37 C.F.R. pt. 201) [hereinafter Librarian Rulemaking].

37. *Id.*

that resides on that handset. In that event, carriers could not combat subscriber churn by selling content to subscribers for download to their handsets and then using handset locks to prevent subscribers from subsequently unbundling the content from their subscriptions.

For a couple reasons, however, the November 2006 rule may have a lesser import than might otherwise seem. First, the rule does not prohibit mobile carriers from continuing to use DRM to lock their handsets, and U.S. mobile carriers show no signs of discontinuing the practice.[38] The rule simply permits reprogramming the handset to use it on a different network. That means that the subscriber must still obtain the knowledge or tools to reprogram the handset or find someone to do it for him. As is apparent from Apple's highly effective use of DRM-laden software updates to render unlocked iPhones into entirely functionless "bricks," that can be no easy task.[39] Moreover, the Librarian of Congress has the authority to suspend just the prohibition on circumvention itself. It remains a violation of the DMCA to provide a "technology, product, service, [or] device . . . that is primarily designed or produced for the purpose of circumventing" an access control measure.[40] Thus, assuming that handset locks in fact qualify as measures that control access to copyrighted works under the DMCA – and we will shortly see how questionable that proposition might actually be – websites that feature handset unlocking software would continue to run afoul of the DMCA trafficking prohibition even if the Librarian rulemaking now permits users to unlock. The same might apply to any mobile carrier or third party that provides the service of unlocking handsets to enable a subscriber to use her handset on a new network.

Second, the Librarian distinguished between circumventing to use a handset on the network of the customer's choosing and circumventing to gain unauthorized access to copyrighted content. As the rulemaking notes, "owners of copyrights in music, sound recordings and audiovisual works whose works are offered for downloading onto cellular phones . . . expressed concern that the proposed exemption might permit circumvention of access controls that protect their works when those works have been downloaded onto cellular phones."[41] The Librarian found that "[t]he record on this issue was fairly inconclusive" and thus,

---

38. *See* Marguerite Reardon, *Will Unlocked Cell Phones Free Consumers?*, C/NET NEWS.COM, Jan. 24, 2007, http://news.com.com/Will+unlocked+cell+phones+free+consumers/2100-1039_3-6152735.html (noting that while a few retailers are beginning to see unlocked handsets, the major mobile carriers continue to limit their subscribers to the locked handsets that the carrier sells).

39. *See* Hafner, *supra* note 13.

40. *See* 17 U.S.C. § 1201(a)(2).

41. Librarian Rulemaking, *supra* note 36, at 68,476.

in essence, that he need not address the issue head-on.[42] He granted the exemption on the assumption that it was "sought for the sole purpose of permitting owners of cellular phone handsets to switch their handsets to a different network," not gain unauthorized access to content.[43]

The Librarian's rule and explanation do not fully answer the question of whether it violates the DMCA to circumvent a carrier's lock on a content-laden handset to enable the subscriber *both* to use the handset with a new carrier *and* continue to have access to the content on the handset. Does the answer depend on the subscriber's primary motive? Or is it the carrier's primary motive – to use DRM to combat subscriber churn as opposed to control access to copyrighted content per se – that matters? Might the Librarian rule differently in three years if carriers and content providers introduce into the record clear evidence that unlocking handsets provides continued, unauthorized access to content residing on the handset?

The Register of Copyright's recommendation to the Librarian to issue the handset lock exemption does little to elucidate this issue. The Register found that copyrighted content can be protected by DRM access controls that are separate from those that lock the handset itself. It noted, indeed, that "the Open Mobile Alliance standard, 'places DRM functionality at a different layer than Service Provider functionality,' and that the 'content industry, in collaboration with the carriers and manufacturers, can simply choose to store the keys to DRMed audiovisual material elsewhere, as is currently the case with many of the handsets on the market.'"[44] The Register also suggested that "a prudent copyright owner of works offered for download to wireless telephone handsets would be wise to insist that access to those works be protected by access controls other than those which control access to the part of the firmware that governs with which wireless communication network the handset will communicate."[45]

However, the Register stopped short of concluding that content providers who rely on the carrier's handset lock, rather than deploying distinct access controls narrowly targeted to their content only, thereby forfeit protection under the DMCA access prohibition. The Register, rather, based her recommendation for the exemption for circumventing

42. *Id.*

43. *Id.*

44. Letter from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress 53 (Nov. 17, 2006) (quoting the oral comments of Jennifer Granick, Stanford Law School, Center for Internet and Society's Cyberlaw Clinic, on behalf of The Wireless Alliance and Robert Pinkerton), *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf [hereinafter Copyright Register 2006 Recommendation].

45. *Id.* at 53 n.157.

handset locks on the absence of evidence in the record that handset locks actually control access to content. As her recommendation stated, "because it appears that there is no reason why those other works cannot be protected by separate access controls, there is no justification for denying an exemption based on speculation that the exemption might permit circumvention that would remove restrictions on access to those works."[46] And the Register recommended tailoring the exemption "so that it does not allow circumvention in order to gain access to copyrighted works, uses of which have not been shown to be noninfringing," suggesting that the exemption should not be available where the handset lock is, in fact, designed to control access to content residing on the handset, whether as a central feature as in the case of iPhone or merely as an intended byproduct of preventing the handset's use in a competing telecommunications network.[47]

The Librarian's rulemaking and Register's recommendation make it clear that the exemption for unlocking handsets does not apply to any DRM that carriers might use to lock content itself, separately from, or in addition to, the handset lock. The 2006 exemption would be unavailable, for example, to circumvent DRM that follows the Apple-AT&T regime of blocking access to content if the mobile handset owner no longer has a subscription with the carrier.

Should such circumvention be otherwise exempted from the DMCA's access prohibition? Say the mobile carrier deploys DRM following the OMA 2.0 standard and configures it not only to protect the content against unauthorized copying, but also to limit its subscribers' ability to switch to other carriers by rendering the content inaccessible upon termination of the bundled subscription. Would and should the Librarian of Congress view that latter use of DRM, like the carriers' handset locks, to reflect "a business decision that has nothing whatsoever to do with the interests protected by copyright"?[48] Does mobile carriers' use of DRM on copyrighted content as a means to combat subscriber churn, over and above protecting the content against unlicensed copying and public distribution, serve the DMCA's purpose of promoting the availability in digital form of "the movies, music, software, and literary works that are the fruit of American creative genius[?]"[49]

In its DMCA rulemaking recommendations, the Register of

46. *Id.* at 53.

47. *Id.* The Register takes what I believe is the correct position that a technological feature or format that inadvertently impedes access does not constitute a "technological protection measure that effectively controls access to a work" within the meaning of the DMCA. Rather the technological impediment must be "imposed in order to control access to a work." *Id.* at 33.

48. Librarian Rulemaking, *supra* note 36, at 68,476.

49. S. REP. No. 105-190, *supra* note 2, at 2.

Copyrights has thus far soundly rejected arguments that consumer circumvention to engage in "space-shifting" of content across devices and formats, such as moving movies from DVDs to one's iPod or moving iTunes music to a non-iPod MP3 player, should be exempted from the access prohibition.[50] In so concluding, the Register has found that exemption proponents have failed to demonstrate that such space-shifting is fair use (which would weigh in favor of an exemption but would not be determinative).[51] The Register has opined, indeed, that "[c]ertainly, where the [unauthorized] online distribution of works is a potential concern, space-shifting will be incompatible with fair use."[52] Supporting that view, the Register has found that DRM tethering of copyrighted works to particular devices and distribution channels has in fact served to guard against the risk of massive illegal distribution and thus promoted greater legal distribution and availability of copyrighted works in digital form.[53]

However, mobile carriers' use of DRM to combat subscriber churn, rather than protect content against piracy, seems distinguishable. Likewise, so does subscribers' circumvention of that DRM to continue to have access to content that the subscriber has purchased and that resides on the subscriber's handset, rather than to space-shift that content to a new device. Almost by definition, this use – and circumvention – of DRM seem to have little to do with interests protected by copyright and everything to do with mobile carriers' communications service business models.

Or do they? As markets and content distribution channels converge, mobile carriers become as much content distributors as providers of telephony and other personal communications services. At some point, their use of DRM to retain subscribers has as much to do with copyright as similar uses by any other content distributor. These include the iPod and iPhone models, as well as the XM Radio/Inno model, under which downloaded music can no longer be accessed when the Inno owner's XM Radio subscription has ceased. They also include the Napster subscription download service whereby, similarly, music downloaded as

---

50. *See* Copyright Register 2006 Recommendation, *supra* note 44, at 69-72.

51. *Id.* at 70. The DMCA provides that nothing in the anti-circumvention provisions "shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1). But that provision stops short of providing a fair use defense to circumvention in violation of the provisions themselves and the Librarian is not required to exempt any uses that are fair uses, but only particular classes of *works* for which the circumvention prohibition adversely impacts persons' ability to make noninfringing uses. *Id.* § 1201(a)(1)(C).

52. *Id.* at 71 (quoting Letter from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress 32 (Oct. 27, 2003), *available at* http://www.copyright.gov/1201/docs/registers-recommendation.pdf).

53. Copyright Register 2006 Recommendation, *supra* note 44, at 71.

part of the Napster subscription is no longer playable if the subscription expires, as well as a host of other subscription services, ranging from online music to cable television, which cease providing access to provider supplied content once the subscription ceases.

DRM access controls in these cases make it possible for content distributors to offer content in various forms and prices. Napster, for example, also sells downloads that purchasers are entitled to keep and play even if they cancel their Napster subscription. These uses of DRM might not aim to prevent unauthorized copying per se; they are access controls, not copy controls. Yet the business models they make possible arguably serve as an incentive for content distributors of various stripes to make digital content more widely available. At least that is an empirical question, and one that touches upon the Librarian's DMCA rulemaking: whether the deployment of DRM is enhancing or impeding socially valuable access to a given category of works. But in a future world in which wireless communications and copyrighted content distribution are integrated within the same markets and services, it should probably not matter for that calculus whether the content distributor is Verizon, Apple, Napster, or Disney.

B. DMCA Case Law

Case law under the DMCA supports a similar conclusion. Manufacturers have used technological protection measures to prevent competition in the aftermarket for spare parts and other related goods and services, ranging from garage door openers to ink cartridges. The technology typically involves software code on interoperating parts that must effect a "handshake" in order for the parts to work with one another. Competitors have in turn devised code to mimic or circumvent that handshake barrier, and some have been sued for circumventing an access control under the DMCA.

The manufacturers have met with little success in these lawsuits; courts have repeatedly found ways to hold that the DMCA does not apply to protect exclusivity in aftermarkets for consumer goods in which manufacturers have embedded computer code. In *Chamberlain Group, Inc. v. Skylink Technology, Inc.*, for example, the Federal Circuit held that the DMCA "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[54] The DMCA, the court stated, was designed to "bring copyright law into the information age," and in so doing, to "maintain balance between the interests of content creators and

54. Chamberlain Group, Inc. v. Skyline Techs., Inc., 381 F.3d 1178, 1202-03 (Fed. Cir. 2004).

information users."[55] The anti-circumvention provisions, the court noted as well, were aimed to implement the World Intellectual Property Organization Copyright Treaty, which requires countries to prohibit "the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights" under copyright treaties.[56] The DMCA applies only when unauthorized access would infringe or facilitate infringement of a copyright. It does not enable a manufacturer to retract consumers' prerogative to use a copy of embedded software in a product they purchased.[57]

A year later, the Federal Circuit declined to extend the DMCA to prevent circumvention of software protection measures designed to provide the plaintiff exclusivity in providing maintenance and repair services for a computer data storage and retrieval system. In so doing, the court reiterated that when "rights under copyright law are not at risk, the DMCA does not create a new source of liability."[58] And, likewise, the Sixth Circuit held that the authentication sequence that a printer manufacturer had embedded in its ink cartridges did not "control access" to the code in the printer and thus could be circumvented without running afoul of the Act.[59]

Applying that precedent, it seems fairly clear that the Librarian of Congress probably did not have to provide an exemption for circumventing handset locks. Circumventing a handset lock that serves only to prevent a mobile phone subscriber from moving to a new network would unlikely be held to violate the DMCA in any event. Like the authentication sequences designed to maintain exclusivity in aftermarket goods and services, mobile carriers' handset locks aim to lock in customers to a business, not protect copyrights or expressive content.

But what if the handset lock served the dual purpose of combating subscriber churn *and* controlling access to copyrighted music, video, and pictures residing on the handset? Or what if the mobile carrier uses the technological control over access to content as an additional means of locking in subscribers? And what if the carrier does so despite the ready availability of DRM that more narrowly protects content against unlicensed copying and distribution when the subscriber moves to a new carrier (something along the lines contemplated by the OMA 2.0 transportability function)? Would the Federal Circuit then view the

55. *Id.* at 1196-97.

56. *Id.* at 1194.

57. *See id.* at 1203.

58. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1318 (Fed. Cir. 2005).

59. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546-47 (6th Cir. 2004).

carrier's use of DRM as one that bears insufficient relation to preventing copyright infringement?

The cases suggest that courts do not require content providers to narrowly tailor their DRM in such a manner. In *Universal City Studios, Inc. v. Corley*, for example, the defendants argued that the software they provided to circumvent the CSS protection on movie DVDs was designed only to enable users of the Linux operating system to play DVDs that they had legitimately purchased. The district court found that contention "immaterial" even if accurate.[60] In upholding the district court's ruling, moreover, the Second Circuit noted that the defendants "offered no evidence that the Plaintiffs have either explicitly or implicitly authorized DVD buyers to circumvent encryption technology to support use on multiple platforms."[61] For the Second Circuit, evidently, the movie studios have the absolute prerogative to use technological protection measures that restrict viewing DVDs to computers with Windows or Apple operating systems, presumably even if Linux compatible DRM were readily available.

In like vein, the Eighth Circuit held in *Davidson & Associates v. Jung* that operators of a website platform for users of Blizzard Entertainment video games to play those games in a multi-player environment without using Blizzard's official multi-player website had violated the DMCA.[62] The defendants were a group of non-profit volunteer game hobbyists, programmers, and others who established their alternative site for playing Blizzard games out of frustration with inadequacies in Blizzard's proprietary site. Significantly for the DMCA claim, Blizzard's official website was constructed to require an authentication sequence "handshake" between an authorized copy of a Blizzard game and the website server in order for the user to enter the site. The defendants' site did not require that "handshake." It automatically allowed all games to be played regardless of whether a game correctly completed the handshake. The Eighth Circuit did not explain how the defendants had thereby circumvented a technological protection measure that controlled access to the plaintiffs' copyrighted games. It did note that the defendants' lack of a requirement that games complete the official "handshake" made it possible for users of illicit copies to play the game in the defendants' multi-player environment.[63] But that did not seem to be the defendants' intention and, in any event, does not mean that the defendants violated the DMCA.

Importantly for our discussion, the defendants reportedly had

60. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 319 (S.D.N.Y. 2000).
61. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001).
62. Davidson & Assocs. v. Jung, 422 F.3d 630, 642 (8th Cir. 2005).
63. *Id.* at 640.

offered to implement an authentication process for their servers to prevent entry to users of illicit copies of Blizzard games.[64] But Blizzard rejected that offer, insisting that it needed to keep its authentication sequence secure.

The *Universal* and *Davidson & Associates* decisions suggest that the DMCA access and trafficking prohibitions will apply even when (1) the defendant circumvents or enables others to circumvent solely to use legitimate copies of copyrighted material on a platform for which the DRM was not designed and (2) the copyright holder could have designed the DRM to be compatible with that platform but chose not to, so long as (3) there is some nexus between the DRM and protecting copyrights. If that reasoning is applied in the mobile carrier arena, it seems that mobile carriers and their copyright holder licensees could use the DMCA to prevent circumvention of DRM that has the effect of locking in subscribers to a particular carrier so long as the DRM also protects copyrighted content from possible illicit copying and distribution. The failure of the mobile carrier and licensee to narrowly target the DRM to prevent only unlicensed copying and distribution, but still allow the subscriber to access purchased content from his or her new mobile communications network, would not give rise to a privilege to circumvent, even solely for the purpose of switching networks. Apple-AT&T could not use the DMCA to prevent subscribers from bypassing a handset lock to use their iPhones on another cellular network. But they could invoke the DMCA against those who seek to hack around whatever DRM software disables the iPhone from accessing iTunes content if the owner's AT&T subscription expires.

II. FEDERAL COMMUNICATIONS COMMISSION

The Federal Communications Commission has the authority to forbid mobile carriers from using DRM to lock in subscribers. Under the Telecommunications Act of 1996, the FCC regulates (or decides not to regulate) to "promote competition and . . . secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[65] The Commission has previously acted to promote competition among telecommunications service providers by mandating number portability. But the Commission declined to prohibit mobile carriers from bundling handsets with service contracts.

---

64. A.H. Rajani, Note, Davidson & Associates v. Jung*: (Re)interpreting Access Controls*, 21 BERKELEY TECH. L.J. 365, 374 (2006).

65. These goals are set forth in the Preamble to the Act. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 15, 18, and 47 U.S.C.).

The FCC considered carriers' bundling of handsets with service contracts in 1992.[66] The Commission conducted its inquiry in light of the prevalent practice of mobile carriers requiring customers to purchase their handsets directly from the carrier or an authorized carrier agent and to contract to pay for a minimum amount of wireless airtime per month over a period of a year or more. In its ruling, the Commission expressed "concern that customers have the ability to choose their own CPE [handset] and service packages to meet their own communications needs and that they not be forced to buy unwanted carrier-provided CPE [handsets] in order to obtain necessary services."[67] The Commission found that while the handset market was fully competitive, the cellular service market was not, thus "leaving open the possibility that bundling may be used for anticompetitive purpose."[68] Nevertheless, the Commission concluded that "the public interest benefits of bundling in the cellular market outweigh the potential for competitive harm."[69] In particular, the Commission found benefit in "the provision of discounted CPE to customers who otherwise would not subscribe to cellular service and the promotion of efficient spectrum utilization by adding new customers to cellular service."[70] It lauded handset discounts as a means of expanding cellular service, given that "the high price of CPE represents the greatest barrier to inducing subscription to cellular service."[71] In its ruling, the Commission permitted carriers to offer handsets and services as a bundled package so long as consumers could still obtain service at a nondiscriminatory price without purchasing a handset from the carrier.[72]

Acting at the direction of Congress four years later, the FCC adopted rules to require both that wireline local exchange carriers offer local number portability for customers who wished to move to a mobile carrier, and that mobile carriers offer number portability for customers who wish to switch mobile carriers or move to a wireline telephone

66. Bundling of Cellular Customer Premises Equip. & Cellular Serv., *Report & Order*, 7 FCC Rcd. 4028, ¶1 (1992).

67. *Id.* ¶ 6.

68. *Id.*

69. *Id.* ¶ 7.

70. *Id.*

71. *Id.* ¶ 19. The Commission's assessment of public interest received indirect judicial support in antitrust litigation against the five largest wireless carriers, in which plaintiffs argued that each defendant's practice of requiring customers to purchase an approved handset constituted an unlawful tying arrangement. In rejecting plaintiffs' claim, the court noted that "wireless service providers continue to package service and handsets, subsidizing the latter, 'to continue to open markets and make it affordable' for consumers to obtain wireless service." In re Wireless Tel. Servs. Antitrust Litig., 385 F.Supp.2d 403, 410 (S.D.N.Y. 2005).

72. Bundling of Cellular Customer Premises Equip. & Cellular Serv., *supra* note 66, at ¶ 30.

company.[73] In essence, pursuant to the Commission's requirement of "service provider portability," carriers were required to enable "end users to retain the same telephone numbers as they change from one service provider to another."[74] And pursuant to the Commission's requirement of "service portability," carriers were required to enable end users to retain their number when changing from one kind of service to another.[75] The Commission determined that number portability gave consumers greater ability to move from one service provider and kind of service to another, and thus promoted greater competition in telecommunications services. As the Commission stated:

> The ability of end users to retain their telephone numbers when changing service providers gives customers flexibility in the quality, price, and variety of telecommunications services they can choose to purchase. Number portability promotes competition between telecommunications services by, among other things, allowing customers to respond to price and service changes without changing their telephone numbers. The resulting competition will benefit all users of telecommunications services.[76]

Under Commission rules, mobile carriers have been required to provide number portability beginning in November 2003.[77] The FCC has found significant wireless number porting since then. Some 20.4 million wireless subscribers ported their numbers to another wireless carrier from December 2003 through December 2005.[78] Nonetheless, the Commission has also found that "the advent of porting in late 2003 did not lead to a significant increase in wireless churn, but did appear to have had a positive impact on service quality by inducing carriers to engage in aggressive customer retention efforts."[79] According to one industry

---

73. Tel. No. Portability, *Second Memorandum Opinion & Order on Reconsideration*, 13 FCC Rcd. 21,204 (1998), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1998/fcc98275.txt; Tel. No. Portability, *First Memorandum Opinion & Order on Reconsideration*, 12 FCC Rcd. 7236 (1997), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1997/fcc97074pdf.html; Tel. No. Portability, *First Report & Order & Further Notice of Proposed Rulemaking*, 11 FCC Rcd. 8352 (1996), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Orders/1996/fcc96286.txt [hereinafter First Portability Order].

74. First Portability Order, *supra* note 73, at ¶ 172.

75. *Id.* ¶ 174.

76. *Id.* ¶ 30.

77. Under the Commission's rules commercial mobile carriers operating the 100 largest Metropolitan Statistical Areas ("MSAs") were required to be providing number portability by November 24, 2003, and those outside the largest MSAs were required to be local number portability-capable by May 24, 2004. FCC 2006 Mobile Services Report, *supra* note 19, at 65.

78. *Id.* at 66.

79. *Id.* at 67.

analyst, such efforts have included "better deals on upgrade handsets, incentives for signing longer contracts, better customer service, and higher network spending."[80] Certainly, the carriers' near universal practice of locking handsets is also a factor in curbing subscriber churn.

How then should the FCC view carriers' use of DRM on content to impose a barrier to subscriber mobility? Should the Commission view it as an undesirable burden on competition, much like the carriers' now-outlawed requirement that subscribers change their phone number in order to move to a new carrier? Or should the Commission view it as a content-equipment-service bundle that might lead to reduced prices for basic cellular phone service and thus expand availability to low-income consumers? Or rather, should the Commission view carriers' use of DRM even to lock in subscribers as a necessary impetus to spurring the transformation of mobile carriers from suppliers of cellular phone service to providers of a broad range of mobile data services, with possible pro-competitive impact on music and multi-channel video programming markets in general?

In the background, on some accounts, the cellular phone service industry has become even less competitive than at the time of the Commissions' 1992 ruling on handset-service bundling. A leading treatise on telecommunications policy, published in 2005, states that competition in that market is "fierce: the overwhelming majority of the population lives in a county served by at least four alternative providers of wireless services."[81] And the treatise concludes: "[t]here is a broad consensus that this competition has made pervasive regulation of the wireless market unnecessary."[82] But industry mergers leave a market that is actually highly concentrated, with four national carriers that dominate the industry. Recent studies conclude that by 2005, a series of mobile carrier mergers had raised the national level Herfindahl-Hirschman Index ("HHI") to 2300 and the mean HHI for local geographical markets for which mobile phone licenses are issued to above 6000.[83] The Department of Justice considers any market with an

---

80. *Id.*

81. JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 261 (2005).

82. *Id.* at 262.

83. Jeremy T. Fox & Hector Perez, *Mobile Phone Mergers and Market Shares: Short Term Losses and Long Term Gains* 7 (Networks, Elec. Commerce, and Telecomms. ("NET") Inst. Working Paper #06-16, 2006), *available at* http://www.netinst.org/Fox2006.pdf; Jeremy T. Fox, *Consolidation in the Wireless Phone Industry* 16 (NET Inst. Working Paper #05-13, 2005), *available at* http://www.netinst.org/Fox2005.pdf. The FCC finds that the average value of HHIs weighted by geographic market population is "only" 2706. But the FCC uses a metric for measuring geographical markets and concentration in those markets that, it admits, tends to "understate systematically the actual level of market concentration." FCC 2006 Mobile Services Report, *supra* note 19, at 13 n.89.

HHI above 1800 to be "highly concentrated".[84] The national market is also characterized by high entry barriers and significant economies of scale.[85] Like other telecommunications industries, therefore, the mobile carrier market has built-in tendencies to oligopoly.[86]

Seen in that perspective, FCC rules to ensure that mobile subscribers may freely move from one carrier to another appear warranted to promote competition in the industry. While subscriber churn is not a good in and of itself, we want mobile carriers to aim to keep existing subscribers by providing better service at lower price, not by using DRM to lock them in. There seems to be a consensus, even among consumer advocates, that government regulation is not needed to force interoperability of devices that play content at this point generally.[87] However, there might be reasons to do so in the highly concentrated mobile carrier industry nonetheless. At the very least, the Commission might require adequate advance notice to subscribers that whatever content they download will be lost if they move to another carrier (if that in fact becomes the business model). In that way, consumers will be able, at least in theory, to take switching costs into account in their decisions to purchase content.[88] As former FCC Chairman Powell has aptly put it: "consumers must receive clear and meaningful information regarding their service plans and what the limits of those plans are. Simply put, information is absolutely necessary to ensure that the market is working."[89]

Yet on the other hand, mobile carriers will very soon find themselves in intense competition with other providers of content and communication. Markets and technology are exerting considerable pressure towards convergence and transportability, a world in which digital content would be seamlessly transportable across platforms within any given media and across different devices and services. In that world, content obtained from any network or source could be accessible through

---

84. U.S. DEP'T OF JUSTICE AND FED. TRADE COMM'N, 1992 HORIZONTAL MERGER GUIDELINES § 1.51(c) (revised in 1997), *available at* http://www.ftc.gov/bc/docs/horizmer.shtm.

85. *See* FCC 2006 Mobile Services Report, *supra* note 19, at 22, 26-38.

86. Eli M. Noam, *Fundamental Instability: Why Telecom is Becoming a Cyclical and Oligopolistic Industry*, 18 INFO. ECON. & POL'Y 272 (2006).

87. *See generally Digital Music Interoperability and Availability: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 109th Cong. 1 (2006).

88. *See generally* Oren Bar-Gill, *Bundling and Consumer Misperception*, 73 U. CHI. L. REV. 33 (2006); Joseph Farrell & Paul Klemperer, Coordination and Lock-in: Competition with Switching Costs and Network Effects (May 2006) (unpublished paper), *available at* http://www.nuff.ox.ac.uk/users/klemperer/Farrell_KlempererWP.pdf.

89. Michael K. Powell, *Preserving Internet Freedom: Guiding Principles for the Industry*, 3 J. ON TELECOMM. & HIGH TECH. L. 5, 12 (2004).

any consumer entertainment or communications device (but, depending on the efficacy and market acceptance of DRM controls, perhaps not freely copied or transferred to others). I could watch a TV program on my computer, handheld media player, or any TV monitor within my home network regardless of whether I have originally accessed or copied the program with my digital video recorder, handheld media player, or computer and regardless of whether the program originates from a broadcaster, webcaster, Internet download site, licensed peer-to-peer (or "superdistribution"), or cellular network. With the growth of Wi-Fi enabled mobile phones, moreover, the mobile carriers' closed communications networks may well face competitive pressure similar to that which will likely overwhelm content distribution and consumption.[90]

In that world of widespread interoperability, competition will focus on which device and service becomes central to consumers. Will it be the mobile carrier multimedia handset and cellular network; handheld Wi-Fi devices capable of Web browsing, Voice-over-IP communication, and receiving music and video webcasting; set-top boxes that can exchange content with other devices on the consumer's network; or any of several other combinations and possibilities?

In the face of that fierce inter-industry competition, mobile carriers will have every incentive to provide premium content in as user-friendly a means and as low a price as possible. There are already reports that "intense competition, coupled with an appreciation of AOL's [failed] walled garden 'experience,' have compelled the [mobile] operators to reduce the costs of accessing the growing range of mobile content."[91] Those cost reductions could well be the first step in the dismantling of the carriers' walled garden models as well.

At the very least, any DRM-backed proprietary platform will have

---

90. *See Martin Defends Draft 700 MHz Band Order as Democrats Express Qualified Support*, TELECOMM. REP. DAILY, July 24, 2007, 2007 WLNR 14155954 (reporting FCC Commissioner Robert McDowell's statement that with the growth of Wi-Fi enabled mobile phones, the walled garden model of the major mobile phone carriers is already starting to dissolve); *see also* Jessica E. Vascellaro & Amol Sharma, *Cellphones Get Wi-Fi, Adding Network Options*, WALL ST. J., June 27, 2007, at B1 (reporting on the immediate promise for mobile carriers, but also the ultimate threat to proprietary networks, posed by Wi-Fi enabled mobile phones). The FCC seems poised to make available vast new spectrum for open communications networks (as well as mobile carriers' proprietary networks), the remaining question being, "how much?" *See* Kim Hart, *Verizon Changes Course, Supports Open-Access Plan*, WASH. POST, July 26, 2007, at D08. That will accelerate Wi-Fi mobile communications competition.

91. Damian Blackden, *The World: How Emerging Markets Drive Mobile Marketing*, CAMPAIGN, July 20, 2007, 2007 WLNR 13882956. On the failure of the proprietary, walled garden business model of AOL, Compuserve, and other early Internet service providers in the face of consumer desire to find information and engage in communication on the wide-open Internet, *see* Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1992-94 (2006).

to provide significant added-value over open networks to remain tenable. To the extent there arises a world of multiple, largely open platforms for communication and content distribution – and whether it arises depends on myriad market, technological, and regulatory developments – a mobile carrier that imposes DRM merely to make it more difficult for subscribers to move to another mobile carrier would quickly find itself surpassed by other platforms, devices, and networks as consumers' first choice for content and communication. Hence, if regulators are concerned about mobile carriers' use of DRM to combat subscriber churn, they might do best to foster the unhindered development and deployment of new, open platforms and to spur greater cross-sectoral interoperability rather than to focus narrowly on a given industry. That way, competition in information platforms will lead to greater availability of content and communications services regardless of some providers' use of DRM to tether content to their particular platform.

CONCLUSION

Following the iPhone's lead, mobile carriers have every temptation to use DRM on the music and video they distribute to lock in subscribers and bolster their walled garden communications networks. At present, their use of DRM in that manner, for that purpose, would likely find enforcement support in the DMCA's anti-circumvention provisions and face no regulatory obstacles at the FCC. At the same time, like Apple, the carriers will face competitive and, possibly, regulatory pressures to provide content that is either DRM-free or transportable across a number of platforms and devices. It is too soon to tell whether, as Wi-Fi enabled mobile devices proliferate, the open Internet will overwhelm the carriers' walled garden networks and force entertainment media to acquiesce in DRM-free content distribution. Much depends on regulatory choice, including the extent to which the FCC makes available new spectrum for open network communication. It is apparent, however, that in the long run, regulators' fostering of a multiplicity of platforms for communication and content distribution, coupled with some degree of cross-platform interoperability, will do more to promote the goals of the Copyright and Telecommunications Acts than would regulation that narrowly targets mobile carriers' use of DRM to combat subscriber churn.

RATIONALIZING INTERNET SAFE HARBORS

MARK A. LEMLEY*

Internet intermediaries – service providers, Web hosting companies, Internet backbone providers, online marketplaces, and search engines – process hundreds of millions of data transfers every day, and host or link to literally tens of billions of items of third party content. They can process and host that data instantaneously[1] only because they automate the process.

Some of this content is illegal. It may infringe copyrights, violate trademarks, disclose trade secrets, defame others, violate privacy rights, contain child pornography, or any of a host of other possible torts or crimes. In the last 12 years, both Congress and the courts have concluded that Internet intermediaries should not be liable for damages for a wide range of content posted or sent through their systems by another.[2] The reasoning behind these immunities is impeccable: if Internet intermediaries were liable every time someone posted problematic content on the Internet, the resulting threat of liability and

* William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP. Thanks to Stacey Dogan, Eric Goldman, Paul Goldstein, Rose Hagan, Ed Lee, Fred von Lohmann, Phil Weiser, and participants in the Digital Broadband Migration conference at the University of Colorado School of Law for helpful comments. I currently represent or have in the past represented various Internet intermediaries, including Google, eBay, and Pacific Bell Internet Services. I also represent plaintiffs seeking redress for online harms in *Doe v. Ciolli*, among other cases. I emphasize that my opinions are my own, not those of my firm or my clients.

1. A search for the word "the" on Google on November 30, 2006 produced approximately 5.8 billion results and took 0.03 seconds. Google Search, The, http://www.google.com/search?hl=en&q=the&btnG=Google+Search (last visited Sept. 17, 2007).

2. *See generally* 15 U.S.C. § 1114(2)(B)-(C) (2000) (trademark); 17 U.S.C. § 512 (2000) (copyright); 47 U.S.C. § 230 (2000) (all causes of action other than intellectual property); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (securities law); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (defamation); Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007) (child molestation by online predator); Chi. Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 681 (N.D. Ill. 2006) (fair housing); Faegre & Benson, LLP, v. Purdy, 367 F. Supp. 2d 1238 (D. Minn. 2005) ("appropriation"); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (defamation); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006) (invasion of privacy); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Cal. Ct. App. 2002) (negligence); Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fla. 2001) (child pornography); Schneider v. Amazon.com, Inc., 31 P.3d 37 (Wash. Ct. App. 2001) (breach of contract).

effort at rights clearance would debilitate the Internet.[3] Google has no realistic way of knowing which of the over 10 billion Web pages it searches might have information on it that violates the rights of someone else. If we forced Google to try to find out which Web pages have problematic materials on them, there is no way it could return automated search results. Even if it employed an army of lawyers to scrutinize all of the content, it would still be in no position to tell which pages were infringing or defamatory.[4] And even if it somehow figured out the answer for any given search result, it would have to determine the answer anew each time the search was run, because Web pages change frequently.

While the logic of some sort of safe harbor for Internet intermediaries is clear, the actual content of those safe harbors is not. Rather, the safe harbors actually in place are a confusing and illogical patchwork. For some claims, the safe harbors are absolute. For others, they preclude damages liability but not injunctive relief. For still others, they are dependent on the implementation of a "notice and takedown" system and a variety of other technical measures. And for at least a few types of claims, there may be no safe harbor at all. This patchwork makes no sense. In this article, I suggest that it be replaced with a uniform safe harbor rule. That suggestion is hopefully uncontroversial. The harder part is deciding what that uniform rule should be. I argue that the best model is the trademark immunity statute, one that lawyers and courts have so far almost completely ignored.

I. THE DIGITAL HOLE IN ISP SAFE HARBORS

The strongest safe harbor, and the one with the broadest applicability, arose largely by accident. In 1996, Congress passed the Communications Decency Act in an effort to make the Internet off limits to adult speech.[5] As part of that Act, Congress responded to concerns that Internet service providers ("ISPs") that took efforts to filter out objectionable content would render themselves liable for defamation as publishers by passing section 230 of the Act. That section provides:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information

3. For a related argument – that search engines deserve special legal protection because they help society deal with information overload through automated sorting of content – *see* Frank Pasquale, *Copyright in an Era of Information Overload: Toward the Privileging of Categorizers*, 60 VAND. L. REV. 135 (2007).

4. I discuss objections to safe harbors, and group or automated responses an intermediary might adopt, below.

5. Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 133 (1996) (codified as amended in scattered sections of 47 U.S.C.).

> provided by another information content provider. . . . No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.[6]

The Communications Decency Act was quickly struck down as unconstitutional.[7] But section 230 survived. Indeed, it flourished. It has been interpreted quite broadly to apply to any form of Internet intermediary, including employers or other companies who are not in the business of providing Internet access[8] and even to individuals who post the content of another.[9] And it has been uniformly held to create absolute immunity from liability for anyone who is not the author of the disputed content,[10] even after they are made aware of the illegality of the posted material[11] and even if they fail or refuse to remove it.[12] The result is that Internet intermediaries need not worry about the legality of the content others post or send through their system, with one significant exception: section 230 does not apply to intellectual property ("IP") claims.[13]

The IP exemption from section 230 creates a gaping digital hole in Internet intermediary immunity. Two statutory provisions partially fill that gap. The first are the copyright safe harbors enacted in the Digital Millennium Copyright Act ("DMCA") in 1998.[14] Those safe harbors create immunity from monetary liability for copyright infringing material posted or sent through an intermediary's system. But they are subject to a number of requirements and limitations. First, unlike section 230, the DMCA safe harbors don't prevent suit for injunctive relief against an

---

6. 47 U.S.C. § 230(c)(1), (e)(3).

7. *See* Reno v. ACLU, 521 U.S. 844 (1997).

8. *See, e.g.*, Delfino v. Agilent Techs., Inc., 145 Cal. App. 4th 790, 804-08 (2006).

9. *See Barrett*, 146 P.3d at 513.

10. *See* cases cited *supra* note 2.

11. *Lycos*, 478 F.3d at 415.

12. *Zeran*, 129 F.3d at 328; Eckert v. Microsoft Corp., No. 06-11888, 2007 WL 496692, at *2-*4 (E.D. Mich. Feb. 13, 2007).

13. 47 U.S.C. § 230(e)(2); *Lycos*, 478 F.3d at 415 (refusing to apply section 230 to a state trademark dilution claim); Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 412-14 (S.D.N.Y. 2001). There are other statutory exceptions as well. For example, violation of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), is exempt from section 230 immunity, as are violations of criminal statutes such as child pornography. *See* 47 U.S.C. § 230(c)(4). And a few courts have refused to apply section 230 in specialized circumstances. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921 (9th Cir. 2007) (refusing to apply section 230 to housing discrimination claims by stretching to find that the intermediary was itself involved in publishing content); Avery v. Idleaire Techs. Corp., No. 3:04-CV-312, 2007 WL 1574269, at *20 (E.D. Tenn. May 20, 2007) (workplace harassment claim based on pornography downloaded on company computers).

14. 17 U.S.C. § 512.

intermediary.[15] Second, they don't protect all Internet intermediaries, but only four classes of intermediaries – conduit providers such as telephone companies,[16] those who store or cache content hosted by another,[17] those who host content posted by another,[18] and search engines.[19] Because those classes were fixed in the statute in 1998, their application to later-developed technologies such as peer-to-peer ("p2p") networks and online marketplaces has not always been clear.[20] Third, most of those protected intermediaries benefit from the safe harbor only if they establish, publicize, and implement both a notice and takedown system for removing all content about which copyright owners complain and a system for identifying "repeat infringers" and kicking them off the system,[21] and only if they accommodate technical protection measures.[22] Finally, the safe harbors for linking and content hosting sites contain a provision that may undo the benefits of the safe harbors altogether. It provides that the safe harbor is unavailable to any site that meets the then-existing legal standards for vicarious infringement.[23] The overall

---

15. *Id.* § 512(j).
16. *Id.* § 512(a).
17. *Id.* § 512(b).
18. *Id.* § 512(c).
19. *Id.* § 512(d).
20. *Compare* A&M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136 (N.D. Cal. 2000) (rejecting section 512 immunity of a company that provided an indexing feature for infringing music supplied by others), *with* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (online auction site qualified for safe harbor as to listings of allegedly infringing copies of movies), *and* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (online marketplace immune from liability for copyright infringement by its vendors).
21. 17 U.S.C. § 512(c)(2)-(3) (notice and takedown); § 512(i)(1)(A) ("repeat infringers").
22. *Id.* § 512(i)(1)(B).
23. *Id.* § 512(c)(1)(B) (safe harbor available only to an intermediary that "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity"). The language suggests that it provides a safe harbor under section 512(c) only against claims of direct and contributory infringement, rather than vicarious liability. The legislative history suggests the opposite. *See* H.R. REP. No. 105-551, pt. 2, at 50 (1998) (suggesting – wrongly – that the bill would "protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement"). And the fact that the statute doesn't use the term vicarious infringement, but instead sets out what were commonly understood in 1998 to be the elements of a vicarious infringement claim, raises additional questions. The Ninth Circuit has steadily whittled away the requirement of "direct financial benefit" as a requirement for vicarious infringement, for instance, to the point where it has held parties liable in the absence of any financial benefit at all, direct or indirect. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); *cf.* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (beginning the whittling away of the "direct financial benefit" requirement completed in *Napster*). And the Supreme Court has created a new tort for inducement of copyright infringement, though it claimed that this new tort was an offshoot of contributory infringement. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). Are these new or broadened torts also outside the safe harbor? A plain reading of the statute would suggest not, but to date there is no case law on the issue.

effect is a set of "safe harbors" that provides something less than perfect safety for intermediaries, and that gives intermediaries incentives to take down any doubtful content as soon as they receive a complaint about it.

Less well-known than the copyright safe harbors is section 32(2) of the Lanham Act,[24] which creates a form of safe harbor from trademark infringement for publishers and extends the definition of publishers to online providers of content written by another.[25] The relevant portions of the statute provide:

> **(B)** Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of Title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125(a) of this title as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.
>
> **(C)** Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 1125(a) of this title with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.[26]

---

24. 15 U.S.C. § 1114(2).

25. *Id.* § 1114(2)(B)-(C).

26. *Id.* While this exclusion applies only to trademark infringement and unfair competition, and not to trademark dilution, a safe harbor for ISPs from the dilution statute is unnecessary because that statute itself provides that they are not liable at all for dilution:

> The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:

This exemption has only rarely been applied by the courts, and seems to be unknown even to many trademark lawyers.[27] It exempts at least some Internet intermediaries – those who are "innocent infringers," a term that is not defined in the Lanham Act – from damages liability, and also from liability for injunctive relief in circumstances where an injunction would interfere with the normal operation of the online publisher. In *Hendrickson v. eBay*, the only case applying this section to the Internet, the court read it to confer broad immunity:

> Plaintiff seeks an injunction enjoining any and all false and/or misleading advertisements that may be posted on eBay's website by users in the future, regardless of whether they are the basis of this lawsuit and whether they have been identified by Plaintiff.
>
> No authority supports Plaintiff's position. Indeed, such an injunction would effectively require eBay to monitor the millions of new advertisements posted on its website each day and determine, on its own, which of those advertisements infringe Plaintiff's Lanham Act rights. As the Court previously noted, "no law currently imposes an affirmative duty on companies such as eBay to engage in such monitoring." . . . eBay has no affirmative duty to monitor its own website for potential trade dress violation and Plaintiff had failed to put eBay on notice that particular advertisements violated his Lanham Act rights before filing suit.[28]

But it is not clear how broadly the exemption applies to Internet intermediaries like backbone providers who are not themselves publishing the content including the trademark. Perhaps they don't need an exemption because they are not engaged in trademark use,[29] but the

---

> (A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
> (i) advertising or promotion that permits consumers to compare goods or services; or
> (ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
> (B) All forms of news reporting and news commentary.
> (C) Any noncommercial use of a mark.

15 U.S.C. § 1125(c)(3). While this language is not a model of clarity, both the reference to use "other than as a designation of source" and to "facilitation" of uses by others would seem to protect ISPs who merely make available the content of others. *Id.*

27. A panel devoted to third-party liability for trademark infringement online at the International Trademark Association meeting did not discuss the section at all, for example.

28. *Hendrickson*, 165 F. Supp. 2d at 1095 (citation omitted).

29. *See, e.g.*, Stacey L. Dogan & Mark A. Lemley, *Grounding Trademark Law Through Trademark Use,* 92 IOWA L. REV. 1669 (2007) [hereinafter Dogan & Lemley, *Grounding*]; Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*,

applicability of the trademark use requirement has been controversial[30] and it is possible that a variety of Internet intermediaries could be sued for direct trademark infringement.

Finally, there is no explicit statutory safe harbor for hosting, transmission, or linking to content that is alleged to violate other types of IP. Internet intermediaries face liability for infringement of patents even if they did not themselves post or authorize the content that turns out to infringe the right. The same may also be true of state IP rights such as the right of publicity and misappropriation of trade secrets, though there is a conflict in the circuits over whether section 230 immunity extends to such state IP rights.[31] It may even be true of violations of the anti-circumvention provisions of the DMCA, if those provisions are read to create secondary liability against those who host or link to anti-circumvention tools.[32] And while the intermediary may have no knowledge of the infringement, that will not protect them from charges of patent or right of publicity infringement because both are strict liability offenses.[33] Nor will it protect them from the occasional claim for direct infringement of other IP rights.[34]

II. STANDARDIZING SAFE HARBORS

A. The Need for Standardization

The patchwork of safe harbors is a result of accident, not design.

---

41 HOUS. L. REV. 777 (2004).

30. *Compare* Graeme B. Dinwoodie & Mark D. Janis, *Confusion Over Use: Contextualism in Trademark Law*, 92 IOWA L. REV. 1597 (2007) (arguing for abolition of the trademark use doctrine), *with* Dogan & Lemley, *Grounding*, *supra* note 29 (defending the doctrine).

31. *Compare Lycos*, 478 F.3d at 418 (assuming that section 230 did not immunize an ISP from liability under a state trademark dilution statute), *with* Perfect10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118-19 (9th Cir. 2007) (holding that "intellectual property" in the exclusion from section 230 immunity means only federal IP rights, not the right of publicity).

32. Whether there is any such theory of secondary DMCA liability is unclear. The DMCA is itself a secondary liability statute, and I am skeptical that tertiary liability – facilitating others whose offense is facilitating still others to infringe copyrights – is or should be a part of the DMCA scheme. But the issue is not free from doubt. *Cf.* Gordon v. Nextel Commc'ns, 345 F.3d 922, 925-27 (6th Cir. 2003) (approving a vicarious liability theory under 17 U.S.C. § 1202 in dealing with alteration of copyright management information).

33. Fla. Prepaid Postsecondary Educ. Expense Bd. v. Coll. Sav. Bank, 527 U.S. 627, 646 (1999) (holding patent infringement does not require proof of intent to infringe); 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 3:27 (2d ed. 2004). Trade secret misappropriation, however, likely requires at least negligence as to the secret status of the information, *see, e.g.*, Cal. Civ. Code § 3426.1(b) (West 2007) (requiring that the defendant knows or has reason to know it is stealing a trade secret), so the risk of liability is lessened there.

34. *See, e.g.*, Complaint at 2-5, Stovall v. Yahoo! Inc., No. 1:07-Civ-00573 (N.D. Ohio Feb. 27, 2007).

The safe harbors arose haphazardly and not always even intentionally. The lack of standardization is problematic for several reasons. First, the absence of any safe harbor for IP infringement other than copyright and trademark (at least outside the Ninth Circuit) creates a hole in the safe harbors, exposing Internet intermediaries to risk of liability and potentially causing them to respond differently to such claims. Second, unsophisticated intermediaries may not be aware of the many nuances in the safe harbors, and may wrongly think they can rely on a safe harbor that does not in fact apply to their circumstance. As a result, they may not react efficiently to charges of infringement. Indeed, I am aware of a number of intermediaries that treat any content-based complaints they receive under the DMCA, whether or not those complaints involve copyrights. Even more likely, unsophisticated plaintiffs and their lawyers may not understand the differences between the safe harbor rules, and therefore file lawsuits that have no chance of success (or decide to forego suits that could in fact be meritorious).

A third problem is the uncertain scope of the IP exception in section 230. We can be quite confident that it applies to patents, copyrights, and trademarks, somewhat less confident that trade secrets and the right of publicity are also IP claims,[35] and even less confident for the penumbra of quasi-IP claims. Cases in this latter category area include the doctrines of misappropriation,[36] idea submission, and state moral rights claims.[37] If all these claims are in fact IP claims, as the First Circuit has assumed,[38] section 230 does not apply and there is no safe harbor at all. If, on the other hand, they are merely state tort claims, as the Ninth Circuit has held with respect to the right of publicity,[39] the absolute immunity of section 230 protects intermediaries.

The inconsistent treatment of different types of claims also leads to litigation abuses by plaintiffs who seek to recast claims subject to significant immunity as different types of claims with lesser or nonexistent immunity. I will give just two examples. First, FedEx threatened an individual who made furniture for his home out of FedEx boxes and put up a Web page at fedexfurniture.com showing pictures of

---

35. *See* Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn From Trademark Law*, 58 STAN. L. REV. 1161, 1163-68 (2006) (describing the history of the right of publicity as a privacy tort rather than an IP right); *cf.* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241 (1998) (challenging the fit of trade secrets within the IP framework).

36. *Cf. Faegre & Benson*, 367 F. Supp. 2d at 1248 (preempting appropriation claim that sounded in IP).

37. *See Perfect10*, 488 F.3d at 1118 ("[S]tate laws protecting 'intellectual property,' however defined, are by no means uniform. Such laws may bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals.").

38. *Lycos*, 478 F.3d at 415.

39. *Perfect10*, 488 F.3d at 1121.

the furniture and how to build it. To the (doubtful) extent that FedEx had any claim at all, it was a trademark claim based on the use of the domain name. But if FedEx asserted only trademark claims, it could not coerce an ISP into taking down the Web site, so it asserted a (entirely bogus) copyright claim instead.[40] Similarly, the husband of a baron in Second Life whose avatar was the subject of an offensive video sent a DMCA copyright notice to YouTube in an effort to have the video removed.[41] The plaintiff might have had a defamation or invasion of privacy claim, but YouTube would have been entirely immune from liability for those claims under section 230. By mischaracterizing tort claims as copyright claims, plaintiffs seek to take advantage of a more favorable legal regime. This sort of gamesmanship is undesirable.

The inconsistencies in the current safe harbors may affect ISP behavior in undesirable ways as well. The stated purpose of section 230 was to give ISPs the freedom to exercise editorial control over content on their sites without being deemed a "publisher" subject to liability for the content choices it makes. But because copyright law has a different rule, exercising that editorial control can be evidence leading to a finding of vicarious liability in a copyright case. As a result, ISPs may be unwilling to establish or exercise any power to excise harmful content from the site even in a tort case covered by section 230, lest doing so take them outside the copyright safe harbor.

Against these arguments for standardization, some might claim that the differential treatment of safe harbors is desirable. Copyright owners, for instance, might allege that copyright infringement is a worse problem than online defamation, and that they should therefore have more power to reach third parties involved somehow in that infringement. But the patchwork of current rules is unlikely to correspond to good policy in particular cases except by accident. Perhaps there is an argument that as a matter of policy there should be complete immunity from right of publicity claims, strong immunity from trademark claims, weaker and conditional immunity for copyright claims, and no immunity from patent claims, but I'm skeptical. More likely, people who benefit from particular rules – ISPs and anonymous defendants in the case of section 230, copyright owners in the case of the DMCA – have come to view those rules as entitlements and to object to anything that changes the status quo. But the fact that we've done it this way for ten years[42] is not

40. *See* Wikipedia, Fed Ex Furniture, http://en.wikipedia.org/wiki/FedEx_furniture (last visited Sept. 17, 2007).

41. *See* Daniel Terdiman, *DMCA Complaint Against YouTube Dropped*, ZDNET NEWS, Jan. 15, 2007, http://news.zdnet.com/2100-9588_22-6150216.html?part=rss&tag=feed&subj=zdnn.

42. It may even be less than ten years. The DMCA was adopted in 1998, but applications of those safe harbors to new technologies came later. And some of the rules are still unclear,

a strong argument that it must always be done this way. In the next section, I discuss some of the problems with particular rules. In the absence of some reason to treat different causes of action differently, there are a variety of benefits to standardization.

B. Standardization on What?

If we are to replace the patchwork of safe harbors in the existing law with a uniform rule covering both IP and other tort claims, what should that rule look like? There are four basic possibilities: no safe harbor at all, complete immunity, a notice and takedown regime modeled on the DMCA, or a no-damages, no-interference regime modeled on the trademark statute. I consider each in turn.

1. No safe harbor

A few scholars have argued for liability for Internet intermediaries, contending that imposing liability on those intermediaries will give them efficient incentives to identify and block infringing or other offensive material.[43] Whatever the abstract merits of this cost-internalization rationale in theory, in practice, I think it is likely to be a disaster. It is simply impossible for a search engine – to say nothing of an ISP or bandwidth conduit – to cull through the literally billions of links and messages they process every day and identify all those messages and Web pages that may create liability under any law. This is not just a technical problem of assessing those petabytes of data, though comparing everything on the Web to everything ever copyrighted in real time is computationally infeasible with existing or any foreseeable technology. Rather, the deeper problem is that there is no way to automate the process of determining legal liability. Software can perhaps strip certain offensive words out of email text, though even the offensiveness of words turns out to be surprisingly contextual, as those who have dealt with Web filtering software have discovered. But there is no way for them to determine whether a message defames another, or violates the securities laws, or invades the privacy of another, or constitutes a trademark use likely to confuse consumers. Image-parsing software may someday be able to identify pictures or videos that are similar to

---

as the *Viacom v. Google* case demonstrates. *See* Complaint, Viacom Int'l Inc. v. YouTube, Inc., No. 1:2007-CV-02103 (S.D.N.Y. Mar. 13, 2007).

43. Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); *see also* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569 (2001). *Cf.* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006) (making a case for ISP liability for viruses and software flaws, but distinguishing copyright infringement).

individual copyrighted works, but they will never be able to determine whether those pictures are fair uses, or whether they are legitimate copies or displays made under one of the many statutory exceptions, or whether the individual pictured is 16 rather than 18 years of age. Add to all of this the fact that it is not just every law in the U.S. but the overlapping, sometimes-inconsistent legal rules of every country that intermediaries would have to apply, and you begin to see the scope of the problem.

Lichtman and Landes acknowledge this problem, but reply that Internet intermediaries don't need to weed out this infringing material; they can simply compensate the universe of all plaintiffs for harm suffered as a result of the Internet, and pass the cost of that compensation on to their users.[44] But that won't work either. To begin, it is worth noting that capping ISP liability at cost internalization is not even possible under the current copyright regime because the Copyright Act provides for a floor of statutory damages ($750 per work) that will often exceed by orders of magnitude the harm actually suffered by copyright owners. If YouTube, eBay, Yahoo!, Verizon, Comcast, and others face the prospect of tens of billions of dollars in statutory damages for hosting, carrying, or linking to content whose provenance they cannot determine, they will either go out of business or they will impose restrictions on the content they will carry sufficiently onerous that they would effectively lock down the Internet. A similar problem results from the fact that the IP rules in particular are commonly protected by property rules. A court that enjoins the display of infringing material may effectively end up enjoining the operation of the Internet intermediary altogether because there is no way for the intermediary to block the infringing material from every source without blocking lots of non-infringing material as well.[45] At a minimum, therefore, treating ISPs as cost aggregators would require elimination of statutory damages rules, punitive damages in tort, and all injunctive relief.

But even as to laws that do limit remedies to compensatory damages – defamation, say – passing liability on to Internet intermediaries will not result in efficiency. Because there is no obvious way for search engines, ISPs, or conduit providers to distinguish infringing from non-infringing content ex ante, those intermediaries cannot simply refuse to deal with infringers. Rather, they will have to serve as "Internet insurers," spreading the risk of all types of harm to all their members. This would create what is arguably the largest moral hazard problem ever seen. If you are paying your ISP thousands of dollars for connectivity because millions of people are using the Internet to trade music for free, you

44. Lichtman & Landes, *supra* note 43, at 404-07.

45. Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783 (2007).

would be a fool not to download your music illegally. Replacing a regime under which tortfeasors are liable with one under which technology companies are liable and tortfeasors can act with impunity seems unlikely to efficiently control tortious behavior.

Finally, there is an even more systematic problem with treating Internet intermediaries as cost-bearers. Intermediaries do not and cannot reasonably expect to capture anything like the full social value of the uses that pass through their system. If we impose the full social costs of harm from third party postings on intermediaries, but they cannot capture the full social benefits of those postings, they will respond by inefficiently restricting the uses that third parties can make of the Internet.[46] Given that Internet access is not the sort of conduct in which the externalized harms significantly exceed the externalized benefits, a strict liability approach of this sort is likely to be inefficient.[47] If we adopt it, the only intermediaries we see are ones that, like cable networks, transmit only pre-approved content from a short list of providers. The amazing diversity of the Internet, with its abundance of user-generated content, would be impossible.

2. Absolute safe harbor

At the opposite end of the safe harbor spectrum is section 230. While that section was arguably intended only to have the limited effect of overruling a few decisions that had treated ISPs as speakers for defamation purposes,[48] courts interpreting it have unanimously read it more broadly, as creating absolute immunity for ISPs and anyone else who is not the author of the content for which liability is asserted. Applying absolute immunity to IP claims as well would certainly solve the liability and moral hazard problems described above. And some will argue that section 230 has worked well for non-IP torts, and so could be expanded to IP cases as well without fear of harm. But I think this approach goes too far in the other direction. Under section 230 today,

---

46. For an economic demonstration of this point, *see* Brett M. Frischmann & Mark A. Lemley, *Spillovers*, 107 COLUM. L. REV. 257 (2007).

47. For a detailed economic analysis along these lines, with particular attention to cybersecurity issues, *see* Keith N. Hylton, *Property Rules, Liability Rules, and Immunity: An Application to Cyberspace*, 87 B.U. L. REV. 1 (2007).

48. *See* H.R. REP. No. 104-458, at 194 (1996) (Conf. Rep.). The particular case that triggered Congressional concern was Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which had held Prodigy strictly liable for republishing a defamatory statement; *see also* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (recognizing a distinction between those who affirmatively publish a libel and those who merely distribute it, and treating ISP as a distributor subject to lesser liability). For a discussion of the legislative history, *see* Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 174-78 (2006).

ISPs have no incentive to police their sites even for content that obviously does not belong there, or to take down even material that is clearly false or injurious. Nor are they even obligated to aid the plaintiff in finding the wrongdoer by disclosing the identity of their clients.[49] As a result, absolute immunity may lead to plaintiffs being unable to remove objectionable material or to find the tortfeasor in order to recover damages from her, and therefore remaining uncompensated even for egregious harms. Expanding this absolute safe harbor to IP cases would be particularly problematic if copyright owners had no way to find the people who were actually cracking their encryption systems and posting their content online.

3. Notice and takedown

The copyright safe harbors built into the DMCA solve these problems by conditioning immunity from liability on an ISP or other intermediary (1) taking down material once the copyright owner has complained of it,[50] (2) identifying its customers once it receives a subpoena,[51] and (3) terminating repeat infringers.[52] The DMCA therefore represents a sort of middle ground between the extremes of no liability and unrestricted liability.

Nonetheless, the DMCA safe harbors have a number of problems. First, they were drafted in 1998 to carve out specific intermediaries, rather than creating a general protection for Internet intermediaries hosting, passing through, or linking to the content of another. As a result, they almost immediately became obsolete as new technologies – most notably p2p networking – were developed. As new business models develop, and as companies in the existing categories change the way they work, the specific categories of the DMCA are likely to be less and less relevant. Thus, a potential advantage of the DMCA approach – the fact that it treats different types of intermediaries differently – has become, over time, a problem instead.

Second, the safe harbor for content hosting companies in section

49. In *Zeran v. America Online*, for example, an anonymous poster offered T-shirts making fun of the Oklahoma City terrorist bombing less than a week after it occurred, and said the T-shirts were available at Zeran's phone number. *Zeran*, 129 F.3d at 329. As a result, Zeran received a constant stream of abusive calls and death threats. *Id.* AOL eventually removed the postings, but never identified the perpetrator. *Id.*

50. 17 U.S.C. § 512(c)(1)(C).

51. *Id.* § 512(h).

52. *Id.* § 512(i)(1)(A). As David Nimmer has pointed out, however, it is not at all clear what it means to be a repeat infringer. David Nimmer, *Repeat Infringers*, 52 J. COPYRIGHT SOC'Y 167 (2005). *Cf.* Mark A. Lemley & R. Anthony Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1 (2005) (offering a middle ground on the issue).

512(c) contains what may turn out to be a gaping loophole – it does not protect any intermediary who is engaged in conduct that the law at that time defined as vicarious infringement.[53] Courts have been expanding the scope of vicarious infringement over time, concluding that "direct financial benefit" required for vicarious infringement could be satisfied without proof of any revenue at all,[54] and that the "ability to control" infringement was satisfied if a landlord or site owner could stop infringement by shutting down the whole system.[55] They have also created an entirely new doctrine of copyright infringement inducement whose status within the indirect liability framework is unclear.[56] A "safe harbor" that opens ISPs to liability whenever a plaintiff can allege that the ISP is making money in part from customer infringement and that it could do more than it does to prevent infringement is a weak shelter indeed.[57]

Finally, the effect of the notice and takedown system has been to encourage Internet intermediaries to take down any and all content copyright owners complain of, no matter how frivolous the complaint.[58] Indeed, a recent study of DMCA takedowns found that 30% of them were legally dubious at best.[59] While the law is even-handed and provides for a mechanism for posters to get their content put back,[60]

---

53. 17 U.S.C. § 512(c)(1)(B) (safe harbor available only to an intermediary that "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity").

54. *A&M Records*, 239 F.3d at 1004.

55. *Id.*; *Fonovisa*, 76 F.3d at 259.

56. *Grokster*, 545 U.S. at 913.

57. Section 512(c) contains other loopholes as well, including one limiting immunity to intermediaries that are "not aware of facts or circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(ii). While it seems reasonably clear that this sort of "red flag" knowledge is intended to apply only to require intermediaries to remove specific content they discover and strongly suspect is infringing – were that not so, this provision would swallow the entire safe harbor – uncertainty about its meaning has allowed Viacom to bring a copyright lawsuit against YouTube and allege that YouTube does not qualify for the safe harbor, despite YouTube's compliance with over 100,000 Viacom DMCA takedown notices. *See* Geraldine Fabrikant & Saul Hansell, *Viacom Tells YouTube: Hands Off*, N.Y. TIMES, Feb. 3, 2007, at C1.

58. On this problem, *see, e.g.*, Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1007-08 (2001). Fred Yen argues that this tendency is exacerbated by the risk of enterprise liability faced by any ISP that doesn't fit within the safe harbors. Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833 (2000). *See generally* Seth F. Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 11 (2006) (referring to efforts to "enlist Internet intermediaries as proxy censors").

59. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006).

60. 17 U.S.C. § 512(g). Significantly, however, only hosting companies have to give

many posters are legally unsophisticated and don't know that they have this right or how to exercise it. Indeed, Urban and Quilter find that very few people avail themselves of this mechanism.[61] Notice and takedown therefore rewards overzealous copyright owners who use the DMCA mechanism to rid the Web even of legitimate content, secure in the expectation that ISPs will take everything down rather than risk their eligibility for the safe harbor.[62] This is a problem in copyright cases, but it's likely to be an even greater problem if a notice and takedown regime is extended to a variety of non-IP tort claims, including such First Amendment-sensitive issues as defamation and invasion of privacy. The notice and takedown approach has been applied outside IP in much of the rest of the world, and the consequences for speech have not been pretty.[63]

4. The trademark regime

An ideal safe harbor would take the middle ground approach of the DMCA, but would avoid some of its pitfalls. It would be general rather than specific in its application to Internet intermediaries. It would give plaintiffs the information they needed to find tortfeasors, and would give them a mechanism for quickly and cheaply removing objectionable content from the Web, but it would also discourage intermediaries from automatically siding with the plaintiff, and would give them real immunity against the specter of damages liability.

I think the trademark immunity statute comes the closest to an ideal approach. It is general in its scope, applying to offline as well as online publishers of content provided by another. It provides a complete immunity from damages liability for intermediaries that are "innocent infringers," and also prevents courts from granting overbroad injunctions that would hamper the operation of the intermediary in an effort to stop one particular act of infringement. It is not conditioned on a regime of automatic takedown, but at the same time it allows plaintiffs to get an

---

their customers notice before taking material down; search engines and caching sites do not.

61. Urban & Quilter, *supra* note 59, at 679-80. They find that fewer than 1% of all takedowns ever receive a putback notice, but that number may be artificially small because so many of the notices in their study were sent to search engines, which have no statutory obligation to notify a site when a search result is removed. *Id.* Even excluding all section 512(d) notices from their study, however, raises the number of putbacks to only 6%. *Id.*

62. There is a provision punishing anyone who "knowingly materially misrepresents" the copyright status of a work in a DMCA notice by subjecting them to liability for attorney's fees. 17 U.S.C. § 512(f). But it has been read narrowly, to exempt even those who have an objectively unreasonable belief in their case. *See* Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000, 1004-05 (9th Cir. 2004). As a result, only one case has actually awarded fees under section 512(f). Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004). *Cf.* Marvel Enters., Inc. v. NCSoft Corp., No. CV-04-9253RGKPLAX, 2005 WL 878090 (C.D. Cal. Mar. 9, 2005) (refusing to dismiss a claim for fees).

63. For a brief discussion, see *infra* notes 73-78 and accompanying text.

injunction removing offensive content.

The trademark model is not perfect, however. Because litigation to an injunction would be costly, it may be that ISPs will still have an incentive to take down content in the face of a threat of suit, so the possibility of overbroad takedowns still exists in the trademark model. And without the notice and putback provisions in the DMCA, that incentive could exacerbate the overdeterrence problem already evident in copyright cases. The solution may be to borrow from another aspect of trademark law – the development of the Uniform Dispute Resolution Process ("UDRP") for resolving cybersquatting complaints. Tony Reese and I have elsewhere proposed a fast, cheap online arbitration for digital copyright disputes,[64] and something along those lines could be expanded to apply to claims made against ISPs for other types of content as well. The law should also include punishments for abuse of the takedown process.[65]

My only other concern with the trademark model is the vagueness of the term "innocent infringers." Were a court to interpret this language to preclude reliance on the safe harbor by anyone who had ever received a trademark complaint, it would undo the benefits of the safe harbor.[66] The legislative history makes it clear that this term is intended instead to invoke the rather strict standard of actual malice from the defamation cases:

> the revision sets forth critical constitutional protections that underlie changes made in section 43(a). It exempts from liability "innocent" disseminators of offending material, whether that material constitutes a violation of section 32(1), relating to infringement, or of proposed Section 43(a), relating to false and misleading commercial advertising. Most prominently, the change protects newspapers, magazines, broadcasters, and other media from liability for the innocent dissemination of commercial false advertising, including promotional material. The word "innocent" is intended to encompass the constitutional standards set forth in New York Times v. Sullivan, 376 U.S. 254 (1964) and its progeny.[67]

Assuming courts apply this standard, as at least one has done,[68] the safe

---

64. Lemley & Reese, *supra* note 52, at 1.

65. The DMCA has such a provision. 17 U.S.C. § 512(f).

66. In *Hendrickson v. eBay, Inc.*, the court did not face this issue, because there was no evidence that the defendant was even aware of the trademark claims before the suit was filed. *Hendrickson*, 165 F. Supp. 2d at 1095.

67. 134 CONG. REC. H31851 (daily ed. Oct. 19, 1988) (statement of Rep. Kastenmeier).

68. NBA Props. v. Untertainment Records LLC, No. 99 CIV 2933(HB), 1999 WL 335147, at *14 (S.D.N.Y. May 26, 1999) ("Adopting that view of the 'innocent' standard, the NBAP would have to prove that Vibe acted either (i) with knowledge that the publication infringed the NBAP's rights, or (ii) with reckless disregard as to whether the Advertisement

harbor should provide effective protection.

One other thing I think needs to be added to the trademark regime is a streamlined subpoena rule along the lines of what the DMCA attempted for copyright law.[69] If plaintiffs are unable to recover damages from Internet intermediaries, it seems only reasonable that they have recourse against the people actually causing the harm. The alternative – requiring a *Doe* lawsuit filed in a random court that may or may not (probably not) have jurisdiction over the defendant – has the advantage that the plaintiff can be forced to demonstrate the strength of its case before discovering the identity of the defendant.[70] But it has the disadvantages that it requires a lawsuit be filed when in many cases the issue could otherwise be resolved without litigation, and that it requires that lawsuit be filed when the plaintiff has no idea where the defendant resides, with the result that the parties are far more likely to engage in unnecessary litigation over personal jurisdiction.[71] An optimal procedure might steer a middle ground, allowing subpoenas upon a showing of good cause even without filing a lawsuit, but requiring the ISP to notify the defendant and give them a chance to anonymously contest the subpoena, either in court or in the sort of online administrative procedure I outlined above.

It is true that requiring intermediaries to retain and disclose the identity of their customers in response to a subpoena will make truly anonymous posting difficult (or even impossible, if no ISP is willing to forego the safe harbor in order to provide its customers with anonymous Internet access).[72] But that price may be worth paying for a system that

---

infringed NBAP's rights.").

69. The actual efficacy of the DMCA subpoena system was significantly weakened by the decisions in In re Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005), and Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003). In the wake of those decisions, copyright owners have had to file *Doe* lawsuits against unknown file sharers, and courts have not been receptive to grouping Does together, making it virtually impossible to pick a court that has jurisdiction over the unknown defendant. For a rare example of a suit against a file sharer that actually went to judgment, *see* BMG Music v. Gonzalez, 430 F.3d 888 (7th Cir. 2005). Congress's goal was to create a streamlined procedure that did not require lawsuits filed against unknown parties, and that goal seems a reasonable one. But after the decisions in *Charter* and *Verizon* it will take legislative change to implement such a procedure.

70. For examples of this procedure under current tort law, *see, e.g.*, Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); In re Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan.31, 2000), *rev'd*, 542 S.E.2d 377 (2001).

71. In some cases, circumstances may suggest that the defendant resides within the jurisdiction. For example, subpoenas to universities are likely to find defendants who reside at or near the university.

72. Under my approach, ISPs who wish to qualify for the safe harbor must keep records of who has posted the material. Other ISPs could opt to provide anonymity to consumers who desire it, as Freenet and Earthstation 5 already do. *See* John Alan Farmer, Note, *The Specter of*

allows redress of real harms without overwhelming ISPs with liability. It is worth noting in this regard that most people who think they have anonymity now do not in fact have it, and that the existing DMCA system effectively requires ISPs to disclose the identity of their customers in copyright cases, a rule that has not led to widespread problems as far as I can tell.

C. International Standardization

Changing U.S. law to standardize on a safe harbor will solve only part of the problem facing Internet intermediaries. Other countries, particularly in Europe, have not yet fully understood the benefit of insulating Internet intermediaries from unreasonable liability, perhaps because the intermediary defendants have largely been American companies and the plaintiffs have all been local. While the EC's 2000 Electronic Commerce Directive[73] provides for some safe harbors, they do not appear to be working, at least as implemented in national legislation and the courts.[74] Those courts have regularly found intermediaries liable for selling Nazi memorabilia,[75] linking to sites containing copyrighted material,[76] or allowing competitors to run advertisements opposite search results.[77] And Europe in particular is contemplating going even further,

---

Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks, 72 FORDHAM L. REV. 725, 726 (2003) (pointing to Freenet as a means for circumventing legal regulation). But the law may render any hope of anonymity on the part of ISP consumers irrelevant; pending federal legislation would require ISPs to keep records of postings so the government could access it. Declan McCullagh, *GOP Revives ISP-tracking Legislation*, CNET NEWS.COM, Feb. 6, 2007, http://news.com.com/2100-1028_3-6156948.html. That legislation would presumably trump the state constitutional right to privacy of ISP data that some courts have recognized. *See* State v. Reid, 914 A.2d 310 (N.J. Sup. Ct. App. Div. 2007). Similar legislation is already in force in other countries. *See, e.g.*, Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services, 2006 O.J. (L105).

73. For a discussion, *see* Rosa Julia-Barcelo, *On-line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks*, 22 EUR. INTELL. PROP. REV. 105 (2000).

74. Part of the problem is that the Directive seems to contemplate ISP liability for negligence in allowing infringing material to be posted. Council Directive 2000/31/EC, art. 14, 2000 O.J. (L178). *See also* Gerald Spindler & Matthias Leistner, *Secondary Copyright Infringement – New Perspectives in Germany and Europe*, 37 INT'L REV. INTELL. PROP. & COMPETITION L. 788, 789 (2006).

75. *See* Yahoo! Inc. v. La Ligue Contre la Racisme et L'Antisemitisme, 433 F.3d 1199, 1201-05 (9th Cir. 2006) (en banc) (discussing the history of the case, in which a French prosecutor charged Yahoo! with maintaining on a US Web site material protected under the First Amendment but illegal under French law).

76. *See, e.g.*, Cybersky, Oberlandesgericht [OLG] [Hamburg Ct. App.] Feb. 8, 2006, docket number 5 U 78/05, at juris online/Rechtsprechung (liability can be premised on a causal connection between the ISP and the illegal content, even though the content was posted by a third party acting autonomously).

77. *See, e.g.*, Viaticum/Luteciel v. Google France, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Nanterre, 2e ch., Oct. 13, 2003, RG No. 03/00051

holding Internet intermediaries criminally liable for IP infringement that occurs on their systems.[78] Even if we rationalize U.S. safe harbors, therefore, intermediaries will still face unreasonable liability outside the United States. To help solve this problem, Congress and the Administration should press for treaty commitments creating international safe harbors along the lines of a rationalized U.S. safe harbor. Without some form of international protection, intermediaries will face unreasonable risks of liability abroad.

CONCLUSION

Internet intermediaries need safe harbors. In the United States, they have such safe harbors for most – though not all – tort claims. But those safe harbors vary widely in their efficacy, sometimes providing too much protection and sometimes too little, and the patchwork quilt of protections leaves significant holes. A single, rationally designed safe harbor based on a modified trademark model would not only permit plaintiffs the relief they need while protecting Internet intermediaries from unreasonable liability, but would also serve as a much needed model for courts in the rest of the world, which have yet to understand the importance of intermediaries to a vibrant Internet.

(holding Google liable for letting advertisers run ads opposite generic terms "flight market" and "travel market" that the plaintiff claimed as trademarks) (appeal pending).

78. *See* Paul Meller, *EU Weighs Copyright Law*, PC WORLD, Mar. 20, 2007, http://www.pcworld.com/printable/article/id,129995/printable.html (discussing EC draft law).

TELECOM GLOBALIZATION AND DEREGULATION ENCOUNTER U.S. NATIONAL SECURITY AND LABOR CONCERNS

WARREN G. LAVEY*

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

* Partner, Skadden, Arps, Slate, Meagher & Flom LLP; Former Assistant to the Chief, Common Carrier Bureau, Federal Communications Commission; B.A., M.S., Harvard University; Diploma Econ., Cambridge University; J.D., Harvard Law School. 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, Viktor Mayer-Schoenberger, Lionel Olmer, 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. An earlier version of this Article is a publication of the Harvard Program on Information Resources Policy.

1. *See Accessing the Communications Marketplace: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 110th Cong. 3 (2007) (written statement of Kevin J. Martin, Chairman, FCC), *available at*

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 U.S.[5] 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,

---

http://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 RESEARCH, CITIGROUP GLOBAL MARKETS, TELECOMMUNICATIONS SERVICES: EMT CONFERENCE AND 4Q PREVIEW - SIGNALS FOR A TELECOM RENAISSANCE? 1 (2007).

2. *See* CATHY HSU, FCC INT'L BUREAU, 2005 SECTION 43.82 CIRCUIT STATUS DATA (2007), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-269605A2.doc (56% growth in use of U.S.-international facilities for international calls, private lines services, and other services from the U.S. in 2005); FCC INT'L BUREAU, 2004 INTERNATIONAL TELECOMMUNICATIONS DATA 1 (2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-264309A1.pdf (minutes of facilities-based and facilities-resale traffic between the U.S. and other countries increased 32.5% from 2003 to 2004).

3. AT&T Inc. and BellSouth Corp. Application for Transfer of Control, *Memorandum Opinion & Order*, 22 FCC Rcd. 5662, 5807 (2007) [hereinafter AT&T/BellSouth Order].

4. Press Release, AT&T Inc., AT&T, BellSouth to Merge: Combination Will Speed Innovation, Competition, and Convergence (Mar. 5, 2006), *available at* http://www.sec.gov/Archives/edgar/data/732713/000095012306002637/y18291e425.htm [hereinafter AT&T/BS Press Release].

5. AT&T/BellSouth Order, *supra* note 3, at 5807.

> 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].

Id.

and suggested that U.S. businesses must look within the nation's borders for obtaining innovative telecom technologies and associated services:

> 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.[6]

This comes after years of battles by the FCC — under both Democratic and Republican administrations — against barriers imposed by the U.S. 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. Concurring Statement of Comm'r Michael J. Copps to the *Memorandum Opinion & Order* in AT&T Inc. and BellSouth Corp. Application for Transfer of Control, 22 FCC Rcd. 5662, 5833 (2007) [hereinafter 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 Comm'r Deborah Taylor Tate to the *Memorandum Opinion & Order* in AT&T Inc. and BellSouth Corp. Application for Transfer of Control, 22 FCC Rcd. 5662, 5826 (2007); Concurring Statement of Comm'r Jonathan S. Adelstein to the *Memorandum Opinion & Order* in AT&T Inc. and BellSouth Corp. Application for Transfer of Control, 22 FCC Rcd. 5662, 5835 (2007). For different views, *see generally* Robert M. Kimmitt, *Why Job Churn is Good*, WASH. POST, Jan. 23, 2007, at A17 (

> 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.

); BUS. ROUNDTABLE, SECURING GROWTH AND JOBS: IMPROVING U.S. PROSPERITY IN A WORLDWIDE ECONOMY (2004), *available at* http://www.businessroundtable.org/pdf/20040330000brsourcing.pdf; GLOBAL INSIGHT (USA), INC., EXECUTIVE SUMMARY: THE COMPREHENSIVE IMPACT OF OFFSHORE IT SOFTWARE AND SERVICES OUTSOURCING ON THE U.S. ECONOMY AND THE IT INDUSTRY (2004), *available at* http://www.itaa.org/itserv/docs/execsumm.pdf; Paul McDougall, *Indian Outsourcer Breaks $1 Billion Quarterly Sales Barrier*, INFORMATIONWEEK, Jan. 16, 2007, *available at* http://www.informationweek.com/outsourcing/showArticle.jhtml?articleID=196901052.

7. *See* WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY (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.

); WHITE HOUSE, THE NATIONAL SECURITY STRATEGY sec. X (2006), *available at* http://www.whitehouse.gov/nsc/nss/2006/sectionX.html ("Globalization presents many opportunities. Much of the world's prosperity and improved living standards in recent years

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 U.S. 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 U.S., 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 U.K.'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 Article reviews three sets of restrictions on foreign controls over and foreign operations of U.S. telecom businesses

---

derive from the expansion of global trade, investment, information, and technology."); FCC INT'L BUREAU, FOREIGN OWNERSHIP GUIDELINES FOR FCC COMMON CARRIER AND AERONAUTICAL RADIO LICENSES (2004); FCC INT'L BUREAU, REPORT ON INTERNATIONAL TELECOMMUNICATIONS MARKETS 2000 UPDATE (2001); Press Release, FCC, Entry into Force of WTO 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 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. Telecomms. Market, *Report and Order and Order on Reconsideration*, 12 FCC Rcd. 23,891 (1997).

8. Tom Krisher, *Chrysler Signs China Car Deal*, WASH. POST, Dec. 29, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/29/AR2006122900526.html; Gordon Fairclough & Jason Leow, *Chery Assembly Deal Makes Chrysler a Model in Exporting from China*, WALL ST. J., July 5, 2007, at A12; *see generally Behind the Asian Outsourcing Phenomenon*, C/NET NEWS.COM, Feb. 21, 2004, http://news.com.com/Behind+the+Asian+outsourcing+phenomenon/2030-1069_3-5162352.html; *The Problem with Made in China*, ECONOMIST, Jan. 11, 2007, *available at* www.economist.com/business/displaystory.cfm?story_id=8515811.

9. *See Power Corp. to Buy Marsh & McLennan's Putnam*, CNBC.COM, Dec. 29, 2006, http://www.cnbc.com/id/16389766.

10. *See* Gabriel Madway, *U.S. Holdings of Foreign Securities Up 21.7% in 2005*, MARKETWATCH, Dec. 29, 2006.

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 (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) ("CFIUS").[11] The other set of restrictions is in the FCC order on the AT&T/BellSouth merger.

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 Article 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.

Section I of this Article 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, Section II 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, Section III describes some foreign responses, reviews, and restrictions. Then, Section IV 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. These vulnerabilities and

11. *See* Omnibus Trade and Competitiveness Act of 1988, tit. V, pt. II, § 5021, 50 U.S.C.A. app. § 2170 (West 2007) (amending Section 721 of the Defense Production Act of 1950) [hereinafter Exon-Florio Provision]; Exec. Order No. 11,858, 40 Fed. Reg. 20,263 (May 7, 1975); Exec. Order No. 12,661, 54 Fed. Reg. 779 (Dec. 27, 1988); Exec. Order No. 12,860, 54 Fed. Reg. 47,201 (Sept. 3, 1993); 31 CFR pt. 800 (2007). CFIUS reviews were revised by legislation following controversies over China National Offshore Oil Corporation's unsolicited bid for Unocal (July 2005) and Dubai Port World's attempt to acquire port facilities in the U.S. (February 2006). Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (codified as amended in scattered sections of 5, 31 U.S.C., and 50 U.S.C. app.) [hereinafter FINSA].

measures are similar to those addressed through the transaction-specific CFIUS reviews that are limited to foreign acquisitions. Finally, Section V presents the conclusion on problems with the U.S. government's actions on the three transactions described in this Article.

This Article 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 risks of deterring foreign investments in the U.S. 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.

I. 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.[12] 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.[13] The increased focus

12. 47 U.S.C. § 151 (2006).

13. *See* 47 U.S.C. §§ 229, 1001-1010; 50 U.S.C. §§ 1801-1811, 1841-46 (2006); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, tit. II, 115 Stat. 272, 278 (codified as amended in scattered sections of 18, 22, 28, 47, 50 U.S.C.).

on national security after September 11, 2001 included actions highlighting the importance of telecommunications carriers in efforts to safeguard the country against terrorists (through wiretaps and call records)[14] 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."[15]

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.[16] 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. (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

---

14. 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 Corp., 441 F. Supp. 2d 899 (N.D. Ill. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006); ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007); Declaration of Candace J. Morey in Support of Plantiffs' Joint Opposition to Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America and to State Secrets and Related Arguments in Verizon's Motion to Dismiss, *In re* Nat'l Sec. Agency Telecomm. Records Litigation, No. MDL 06-1791 VRW (N.D. Cal. Aug. 30, 2007), *available at* http://www.eff.org/legal/cases/att/06222007_morey_dec.pdf.

15. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE iii (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf [hereinafter NATIONAL STRATEGY]; *see also* FINSA, *supra* note 11, at § 4 (directing CFIUS to consider the potential national security-related effects on United States critical infrastructure caused by foreign acquistitions of domestic businesses); sources cited *infra* note 32.

16. *See* Exon-Florio Provision, *supra* note 11; Henry M. Paulson, U.S. Sec'y of the Treasury, Remarks at Forum on International Investment (May 10, 2007), *at* http://www.treasury.gov/press/releases/hp398.htm [hereinafter 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.

).

acquisition of a 61 percent interest in Global Crossing (2003).[17]

In mid-2006, CFIUS was operating in a highly-charged political environment surrounding its reviews of numerous 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.[18] There was focus on a bid by the government-backed China National Overseas Oil Corporation for Unocal, which was withdrawn after an outpouring of Congressional opposition.[19] The General Accountability Office released a negative report on the thoroughness of CFIUS's reviews and conditions it imposed on transactions.[20] Finally, both houses of Congress were considering numerous bills to revise the standards and review processes for foreign acquisitions, resulting in enactment of the Foreign Investment and National Security Act of 2007.[21]

---

17. *See* James A. Lewis, *New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception*, 57 FED. COMM. L.J. 457 (2005).

18. *See* Jessica Holzer, *Was the Law Followed on Dubai Ports Deal OK?*, FORBES, Feb. 23, 2006, *available at* http://www.forbes.com/business/2006/02/22/logistics-ports-dubai-cx_jh_0223cfius.html; Stephanie Kirchgaessner & James Boxell, *Fear Grows Over New Dubai Revolt*, FIN. TIMES, Mar. 21, 2006, *available at* http://www.ft.com/cms/s/c8f7de22-b91c-11da-b57d-0000779e2340.html; *Key Questions About the Dubai Port Deal*, CNN.COM, Mar. 6, 2006, http://www.cnn.com/2006/POLITICS/03/06/dubai.ports.qa/index.html.

19. *See* DICK K. NANTO ET AL., CONG. RESEARCH SERV., CHINA AND THE CNOOC BID FOR UNOCAL: ISSUES FOR CONGRESS (2005), *available at* http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-7905:1; Matthew R. Byrne, Note, *Protecting National Security and Promoting Foreign Investment: Maintaining the Exon-Florio Balance*, 67 OHIO ST. L.J. 849 (2006); Gaurav Sud, Note, *From Fretting Takeovers to Vetting CFIUS: Finding a Balance in U.S. Policy Regarding Foreign Acquisitions of Domestic Assets*, 39 VAND. J. TRANSNAT'L L. 1303, 1319-26 (2006); Stephanie I. Cohen, *Lawmakers Rip CNOOC's Unocal Bid*, MARKETWATCH, July 13, 2005; David Barboza, *China Backs Away from Unocal Bid*, INT'L HERALD TRIB., Aug. 3, 2005, *available at* http://www.iht.com/articles/2005/08/02/business/unocal.php.

20. U.S. GEN. ACCOUNTABILITY OFFICE, DEFENSE TRADE: ENHANCEMENTS TO THE IMPLEMENTATION OF EXON-FLORIO COULD STRENGTHEN THE LAW'S EFFECTIVENESS (2005), *available at* http://www.gao.gov/new.items/d05686.pdf; *see also* UNITED STATES GEN. ACCOUNTABILITY OFFICE, DEFENSE TRADE: NATIONAL SECURITY REVIEWS OF FOREIGN ACQUISITIONS OF U.S. COMPANIES COULD BE IMPROVED (2007), *available at* http://www.gao.gov/new.items/d07661t.pdf [hereinafter GAO 2007 Report].

21. *See* FINSA, *supra* note 11; *Reform of National Security Reviews of Foreign Direct Investments Act: Hearing on H.R. 5337 Before the Subcomm. on Domestic and International Monetary Policy, Trade, and Technology of the H. Comm. on Financial Servs.*, 109 Cong. (2006) (prepared statement of Clay Lowery, Assistant Sec'y for Int'l Affairs, U.S. Treasury Dep't), *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."); Stephanie Kirchgaessner, *CFIUS Overhaul Back in Spotlight*, FIN. TIMES, Aug. 23, 2006, *available at* http://www.ft.com/cms/s/1523f970-32d0-11db-87ac-0000779e2340.html; Bill McConnell, *Battle Likely After Rival Bills for Foreign Merger Oversight Reform Approved*, THEDEAL.COM, July 28, 2006, *available at* http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1153991138266; Stephen J. Canner, *A Layman's Guide to CFIUS Reform*, POL'Y ADVOC. (U.S. Council for Int'l Bus., New York,

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),[22] and (B) the merger of Lucent Technologies, Inc. and Alcatel (a French company).[23]

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

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.[24] The provisions of this agreement illustrate a broad, penetrating role for these executive branch agencies and a nationalistic approach, which conflicts with 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 (which is treated as part of the U.S. for purposes of CFIUS and FCC jurisdiction).[25]

N.Y.), July 2006, *available at* http://www.uscib.org/index.asp?documentID=3506; Robert M. Kimmitt, Deputy Sec'y of the Treasury, Remarks at the European Institute Luncheon CFIUS Reform and International Investments: Balancing Security and Investment (Oct. 27, 2006), *available at* http://www.ustreas.gov/press/releases/hp155.htm.

22. *See* América Móvil, S.A. de C.V., Verizon Commc'ns 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, *Public Notice*, 21 FCC Rcd. 6492 (2006); Press Release, Verizon Commc'ns Inc., Verizon to Sell Caribbean and Latin American Telecom Operations in Three Transactions Valued at $3.7 Billion (Apr. 3, 2006), *available at* http://investor.verizon.com/news/view.aspx?NewsID=731.

23. *See* Press Release, Alcatel-Lucent, Alcatel and Lucent Technologies to Merge and Form World's Leading Communication Solutions Provider (Apr. 2, 2006), *available at* http://www.home.alcatel.com/vpr/fullarchive.nsf/Datekey/02042006uk [hereinafter Alcatel/Lucent Announcement].

24. Petition to Adopt Conditions to Authorizations and Licenses in Verizon Commc'ns, Inc., Transferor and América Móvil, S.A. de C.V., Transferee, WT Dkt. No. 06-113 (filed Dec. 15, 2006), *available at* http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518713387 [hereinafter TELPRI Security Agreement]. This agreement is attached as Appendix B to the FCC's order approving the transaction. *See* Verizon Commc'ns, Inc., Transferor, and América Móvil, S.A. de C.V., Transferee, Application for Auth. to Transfer Control of Telecomunicaciones de Puerto Rico, Inc., *Memorandum Opinion & Order & Declaratory Ruling*, 22 FCC Rcd. 6195, 6230 (2007) [hereinafter Verizon/AM Order].

25. Overview of Transaction/Petition for Declaratory Ruling/Request for Procedural

América Móvil served approximately 100 million wireless 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.[26]

In applying to the FCC for approval of the transaction, América Móvil claimed that it "will be able to take advantage of economies of scope and scale with its existing operations in serving Puerto Rico."[27] 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.[28] Moreover, it is common for carriers serving multiple

---

Considerations in Applications of Verizon Commc'ns Inc., Transferor, and América Móvil, S.A. de C.V., Transferee, WT Dkt. No. 06-113 (filed May 9, 2006), *available at* http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518360185, http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518360186 [hereinafter TELPRI Application].

26. *Id.* at Overview of the Transaction 4; *Id.* at Public Interest Statement 3.

27. *Id.* at Public Interest Statement 1, 3-5.

28. *See* América Móvil, S.A. de C.V., Annual Report (Form 20-F), at 32 (June 30, 2006), *available at* http://www.sec.gov/Archives/edgar/data/1129137/000119312506140183/d20f.htm [hereinafter América Móvil 2005 Form 20-F] ("Speedy Móvil, 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."); Telefónica Móviles, S.A., Annual Report (Form 20-F), at 79 (Apr. 12, 2006), *available at* http://sec.edgar-online.com/2006/04/12/0001193125-06-078410/Section6.asp ("We are capitalizing on the regional management of operations in the region, the integration of operators acquired from BellSouth, our larger scale and Group know-how to enhance operating efficiency across our operations in Latin America."); SunCom Wireless, Inc., Annual Report (Form 10-K), at 7 (Mar. 16, 2006), *available at* http://www.sec.gov/Archives/edgar/data/1064735/000119312506056246/d10k.htm (carrier providing wireless services in the southeastern U.S., Puerto Rico, and U.S. Virgin Islands; "Our network monitoring system provides around-the-clock surveillance of our entire network."); Centennial Commc'ns Corp., Amendment to Registration Statement (Form S-4/A), at 76-77 (Oct. 1, 2004), *available at* http://www.sec.gov/Archives/edgar/data/879573/000095012304011679/y94431a1sv4za.htm [hereinafter 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.

regions in a country to implement centralized network operating, customer service, switching, Internet peering, and hosting centers as well as other consolidated operations.[29]

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 ("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.[30] The Security Agreement recites several reasons why the CFIUS agencies sought restrictions in connection with the foreign

---

> . . . .
>
> . . . 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.

).

29. *See* Dobson Commc'ns Corp., Annual Report (Form 10-K), at 4, 10, 12 (Mar. 16, 2006), *available at* http://www.sec.gov/Archives/edgar/data/1035985/000095013406005299/d33891e10vk.htm (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 our vendors, who provide monitoring on a real-time basis for items, including alarm monitoring, power outages, tower lighting problems and traffic patterns.

); Centennial, *supra* note 28, at 43 (wireless operations in Indiana, Michigan, Texas, Louisiana and Mississippi, with one centralized customer service center and local customer support facilities).

30. *See* TELPRI Security Agreement, *supra* note 24. 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. *See* Dept. of Def. to Adopt Conditions, Verizon Commc'ns Inc., Transferor, and América Móvil, S.A. de C.V., Transferee, WT Dkt. No. 06-113 (filed Dec. 19, 2006), *available at* http://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* note 24, at 6266.

acquisition of TELPRI, including:

> 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.[31]

Put differently, the U.S. Government appears to be concerned that the foreign owner of the telecom services provider could do any of the following: (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 ability to carry out such adverse activities through the foreign storage of call-related information or foreign routing of traffic.[32]

---

31. TELPRI Security Agreement, *supra* note 24, at 5.

32. *See* DEP'T OF HOMELAND SEC., COMMUNICATIONS: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PLAN 36 (2007), *available at* http://www.dhs.gov/xlibrary/assets/Communications_SSP_5_21_07.pdf [hereinafter COMMUNICATIONS SECTOR PLAN]; DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 107-21 (2006), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [hereinafter NATIONAL INFRASTRUCTURE PROTECTION PLAN]; GAO 2007 Report, *supra* note 20, at 9 ("According to officials from [the Departments of Defense and Justice], [national security] vulnerabilities could result from

To address these concerns, the Security Agreement includes the following commitments:[33]

- All equipment used to transmit, switch, control, manage or supervise "domestic" communications (calls between points in the U.S., 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 U.S., and there shall be no remote access outside the U.S. 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;
- 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

---

foreign control of critical infrastructure, such as control of or access to information traveling on networks."); WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY 17 (1999), *available at* http://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* note 15; Lewis, *supra* note 17, at 468-71; Mark Landler & John Markoff, *In Estonia, What May Be the First War in Cyberspace*, INT'L HERALD TRIB., May 28, 2007, *available at* http://www.iht.com/articles/2007/05/28/business/cyberwar.php.

33. TELPRI Security Agreement, *supra* note 24, at 11-21.

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.[34] 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, and other company operations would be approximately $6.5 million in the first year and $2.5 million in each subsequent year.[35]

---

34. *See* 15 U.S.C. § 16(e) (2006) (applicable to negotiated antitrust constent decrees); United States v. Microsoft Corp., 56 F.3d 1448, 1458-62 (D.C. Cir. 1995); United States v. SBC Commc'ns, Inc., 489 F. Supp. 2d 1 (D.D.C. 2007); United States v. Am. Tel. & Tel. Co., 552 F. Supp. 131, 151 (D.D.C. 1982), *aff'd sub nom*. Maryland v. United States, 460 U.S. 1001 (1983) [hereinafter Divestiture]; *see also* Verizon/AM Order, *supra* note 24, at 6226-27 (FCC accords deference to Executive Branch expertise on national security and law enforcement issues); KENNETH J. ARROW ET. AL, BENEFIT-COST ANALYSIS IN ENVIRONMENTAL, HEALTH, AND SAFETY REGULATION (1996), *available at* http://www.aei-brookings.org/publications/abstract.php?pid=53; ROBERT W. HAHN & ROBERT E. LITAN, IMPROVING REGULATORY ACCOUNTABILITY (1997), *available at* http://www.aei-brookings.org/admin/authorpdfs/page.php?id=202; OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, 2006 REPORT TO CONGRESS ON THE COSTS AND BENEFITS OF FEDERAL REGULATIONS AND UNFUNDED MANDATES ON STATE, LOCAL, AND TRIBAL ENTITIES (2006), *available at* http://www.whitehouse.gov/omb/inforeg/2006_cb/2006_cb_final_report.pdf; Jerry Ellig, *Costs and Consequences of Federal Telecommunications Regulations*, 58 FED. COMM. L.J. 37 (2006).

35. Global Crossing Ltd., Annual Report (Form 10-K), at 10 (Dec. 8, 2003), *available at* http://www.sec.gov/Archives/edgar/data/1061322/000119312503090817/0001193125-03-090817.txt.

> 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

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 ("Communications Act") and FCC orders.

a. 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:

> 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 regulation . . . .[36]

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."[37] 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 preserve 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."[38]

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

---

> incremental expenditures will be approximately $6.5 million in 2004 and approximately $2.5 million in subsequent years; however, the actual costs could significantly exceed these estimates.

Id.

36. 47 U.S.C. § 230(b); *see also* Vonage Holdings Corp. Petition for Declaratory Ruling Concerning an Order of the Minn. Pub. Utils. Comm'n, *Memorandum Opinion & Order*, 19 FCC Rcd. 22,404, 22,416-17 (2004), *aff'd sub nom.* Minn. Pub. Utils. Comm'n v. F.C.C., 483 F.3d 570 (8th Cir. 2007) ("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.'").

37. Telecommunications Act of 1996 § 706(a), 110 Stat. 56, 153 (current version at 47 U.S.C. § 157).

38. Appropriate Framework for Broadband Access to the Internet Over Wireline Facilities, *Policy Statement*, 20 FCC Rcd. 14,986, 14,988 (2005) [hereinafter Internet Policy].

global electronic commerce."[39] 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 following: "(A) the development of telecommunications infrastructure; (B) the procurement of telecommunications equipment; (C) the provision of Internet access and telecommunications services; and (D) the exchange of goods, services, and digitalized information."[40]

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 U.S. Its handling of Internet traffic between two points in the U.S. must solely use facilities in the U.S., and it must provide to the U.S. government descriptions of its facilities. It must manage in the U.S. its network used to transmit Internet traffic originating or terminating in the U.S. Additionally, it must not store outside of the U.S. its customer and traffic records for Internet services provided to U.S. customers.[41]

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.[42] 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.[43] Furthermore,

---

39. Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1998, tit. XII, § 1203(a), 112 Stat. 2681, 2681-727 (1998) (current version at 19 U.S.C. § 2241 (2006)).

40. *Id.* at § 1203(b).

41. In January 2007, in connection with a CFIUS review, 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 in Impsat Fiber Networks, Inc., Transferor, and Global Crossing Ltd., Transferee, WC Dkt. No. 06-215 (filed Feb. 1, 2007), *available at* http://svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518724528, http://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. Domestic 214 Authorization Granted: Application Filed for the Transfer of Control of Impsat USA, Inc. from Impsat Fiber Networks, Inc. to Global Crossing Ltd., *Public Notice*, 22 FCC Rcd. 2491 (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 Ltd., *Order & Authorization*, 18 FCC Rcd. 20,301, app. D (2003).

42. América Móvil, *supra* note 28, at 22; Teléfonos de México, S.A. de C.V., Annual Report (Form 20-F), at 19, 37, 38 (June 30, 2006), *available at* http://www.secinfo.com/d14D5a.v48G7.htm.

43. *See* Peter Burrows, *Servers as High as an Elephant's Eye*, BUS. WEEK, June 12,

these conditions are not generally applicable to providers of Internet services in the U.S., including those against which TELPRI competes.

b. 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.[44] 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.[45] 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 U.S. The Security Agreement bars the likely potential to reduce costs by utilizing network operating centers, lines, or switches outside of the U.S. Such restrictions can impair the efficiency of the carrier's operations and its ability to deploy advanced services.

c. 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.[46] Such economies can yield various public benefits including lower prices to users, increased ability to invest in infrastructure upgrades, greater

---

2006, *available at* http://www.businessweek.com/magazine/content/06_24/b3988087.htm; Stephanie N. Mehta, *Behold the Server Farm*, FORTUNE, July 28, 2006, *available at* http://www.money.cnn.com/2006/07/26/magazines/fortune/futureoftech_serverfarm.fortune/index.htm; *Telemex Will Offer Integrated Services of "Hosting" in Seven Countries*, TERRA, Nov. 14, 2006, *at* http://www.terra.com/noticias/articulo/html/act647858.htm#.

44. *See* 47 U.S.C. § 214(a).

45. *See* Am. Tel. & Tel. Co. v. F.C.C., 978 F.2d 727 (D.C. Cir. 1992); Policy and Rules Concerning the Interstate, Interexchange Marketplace, *Second Report & Order*, 11 FCC Rcd. 20,730 (1996); Policy and Rules Concerning Rates for Competitive Common Carrier Servs. and Facilities Authorizations Therefor, *Fourth Report & Order*, 95 F.C.C.2d 554 (1983); Long-Run Regulation of AT&T's Basic Domestic Interstate Servs., *Notice of Inquiry*, 95 F.C.C.2d 510, 521-23 (1983).

46. *See* Verizon Commc'ns Inc. and MCI, Inc. Applications for Approval of Transfer of Control, *Memorandum Opinion & Order*, 20 FCC Rcd. 18,433, 18,533-35 (2005) [hereinafter Verizon/MCI Order].

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.[47] 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 the following aspects of TELPRI's network: (1) network operating centers and network planning; (2) data processing and storage equipment and operations; and (3) billing and other customer services. The loss of economies of scale and scope could lessen the public benefits ordinarily associated with such a merger.

d. 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.[48] 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 by, among other things, 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.[49]

In contrast, the Security Agreement implements new regulatory burdens on one foreign-owned carrier.[50] These burdens include personnel screening, annual security audits, information storage requirements, information storage restrictions, and reporting requirements.

An argument could be made that the national-security rationale for

47. *Id.* at 18,531-33.

48. 47 U.S.C. § 161.

49. *See, e.g.*, Covad Commc'ns Co. v. F.C.C., 450 F.3d 528 (D.C. Cir. 2006); Unbundled Access to Network Elements, *Order on Remand*, 20 FCC Rcd. 2533 (2004) [hereinafter Unbundled Access]; Implementation of Further Streamlining Measures for Domestic Section 214 Authorizations, 17 FCC Rcd. 5517 (2002).

50. The Security Agreement includes conditions not imposed in the earlier CFIUS agreements with Deutsche Telekom in the VoiceStream Wireless transaction, *see* Applications of VoiceStream Wireless Corp., PowerTel, Inc., Transferors, and Deutsche Telekom AG, Transferee, *Memorandum Opinion & Order*, 16 FCC Rcd. 9779 (2001) [hereinafter DT], or with Telmex in its proposed transaction with XO Communications, *see* Petition to Adopt Conditions to Authorizations and Licenses, XO Commc'ns, Inc., IB Dkt. No. 02-50 (filed Sept. 16, 2002), *available at* http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513291830.

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,[51] and it has broad statutory authority to adopt regulations, or impose conditions on licenses and authorizations, for telecom carriers.[52] 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.[53]

---

51. *See* 47 U.S.C. § 151 (purpose of FCC regulations includes national defense and promoting safety of life and property). For descriptions of some of the FCC's post-9/11 actions to promote national defense and public safety, see *CyberSecurity: Protecting America's Critical Infrastructure, Economy, and Consumers: Hearing Before the Subcomm. on Telecomms. and the Internet of the H. Comm. on Energy and Commerce*, 109th Cong. (2006) (written statement of Kenneth P. Moran, Director, Office of Homeland Sec., Enforcement Bureau, FCC), *available at* http://www.fcc.gov/ola/docs/moran091306.pdf; *Public Safety Communications from 9/11 to Katrina: Critical Public Policy Lessons: Hearing Before the Subcomm. on Telecomms. and the Internet of the H. Comm. on Energy and Commerce*, 109th Cong. (2005) (written statement of Kevin J. Martin, Chairman, FCC), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261417A1.pdf; *Emergency Warning Systems: Ways to Notify the Public in the New Era of Homeland Security, Hearing of the Subcomm. on Emergency Preparedness and Response Before the H. Select Comm. on Homeland Sec.*, 108th Cong. (2004) (written statement of James A. Dailey, Director, Office of Homeland Sec., Enforcement Bureau, FCC), *available at* http://www.fcc.gov/homeland/documents/dailey092204.pdf.

52. *See* 47 U.S.C. §§ 214(c), 219, 220, 301, 303(r); F.C.C. v. Nat'l Citizens Comm. for Broad., 436 U.S. 775 (1978); United States v. Midwest Video Corp., 406 U.S. 649 (1972) (FCC's ancillary jurisdiction); United States v. Sw. Cable Co., 392 U.S. 157, 177-78 (1968) (same); Atl. Tel-Network, Inc. v. F.C.C., 59 F.3d 1384, 1389 (D.C. Cir. 1995) (FCC could impose condition on license even if no such formal policy existed when the condition was imposed); 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 Gen. Commc'n, Inc., *Memorandum Opinion & Order*, 21 FCC Rcd. 14,863, 14,915-16 (2006) (adopting conditions restricting access to business records and other information); *see generally* Bryan N. Tramont, *Too Much Power, Too Little Restraint: How the FCC Expands its Reach Through Unenforceable and Unwieldy "Voluntary" Agreements*, 53 FED. COMM. L.J. 49 (2000).

53. *See infra* Section IV.C.

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

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.[54] 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 before January 1, 1984.[55] 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.[56] Lucent also owned Bell Laboratories, which was a leading telecom research and development organization based in New Jersey. With operations in the U.S. and several foreign countries, Bell Labs performed work for Lucent's commercial products as well as projects for the U.S. government.[57]

The telecom equipment industry and Lucent have changed dramatically since the days of Western Electric's role in the vertically integrated, monopoly Bell System. In the earlier era, Western Electric operated twenty-three major plants scattered around the U.S. and focused on supplying the domestic operations of the Bell System.[58] Through

---

54. Press Release, Alcatel-Lucent, Alcatel and Lucent Complete Merger Creating World's Leading Communication Solutions Provider (Nov. 30, 2006), *available at* http://www.alcatel-lucent.com (2006 Archive of Press Releases); Alcatel/Lucent Announcement, *supra* note 23. 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.

55. Alcatel-Lucent, Lucent Timeline, http://www.bell-labs.com/history/lucent.html (last visited Oct. 7, 2007).

56. *Id.*; Divestiture, *supra* note 34. 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.

57. Alcatel-Lucent, Research Areas & Projects, http://www.alcatel-lucent.com/wps/portal/BellLabs (follow "World-Class Research" hyperlink) (last visited Oct. 7, 2007); Alcatel-Lucent, Global Labs, http://www.alcatel-lucent.com/wps/portal/BellLabs (follow "Global Labs" hyperlink) (last visited Oct. 7, 2007).

58. JOHN BROOKS, TELEPHONE: THE FIRST HUNDRED YEARS 12 (1976); ALVIN VON AUW, HERITAGE & DESTINY: REFLECTIONS ON THE BELL SYSTEM IN TRANSITION 200-08 (1983) [hereinafter VON AUW]; Jerry A. Hausman, *The Bell Operating Companies and AT&T Venture Abroad While British Telecom and Others Come to the United States*, *in*

regulatory and antitrust decisions as well as other market developments, the industry and Lucent became global.[59] 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.[60]

Prior to the merger, both Alcatel and Lucent were operating in the U.S. as well as globally.[61] Neither company provided telecom or Internet services in the U.S. Instead, 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 U.S. 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 U.S. As global suppliers, each company also sold some products outside the U.S. which were, in large part, developed, manufactured and supported by its operations in the U.S.

In announcing the merger, the companies pointed to "a strategic fit between two experienced and well-respected global communications

---

GLOBALIZATION, TECHNOLOGY, AND COMPETITION: THE FUSION OF COMPUTERS AND TELECOMMUNICATIONS IN THE 1990S 313, 314 (Stephen P. Bradley et al. eds., 1993).

59. Divestiture, *supra* note 34; Am. Tel. & Tel. Co., 64 F.C.C.2d 1, 26-45 (1977) [hereinafter FCC Docket 19129]; VON AUW, *supra* note 58, at 200-08; Lucent Techs. Inc., Amendment to Registration Statement (Form S-1/A) (Apr. 1, 1996) (discussion of competition and markets).

60. *See* Lucent Techs. Inc., Annual Report (Form 10-K), at 6 (Dec. 14, 2005) [hereinafter Lucent 2005 Form 10-K]; INT'L TELECOMM. UNION, WORLD TELECOMMUNICATION DEVELOPMENT REPORT 1996/97: TRADE IN TELECOMMUNICATIONS (1998); ORG. FOR ECON. CO-OPERATION AND DEV., TELECOMMUNICATIONS EQUIPMENT: CHANGING MARKETS AND TRADE STRUCTURES (1991), *available at* http://www.oecd.org/dataoecd/56/54/1909439.pdf.

61. Lucent 2005 Form 10-K, *supra* note 60, 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 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, Annual Report (Form 20-F), at 19 (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.

).

leaders who together will become the global leader in convergence" for next-generation networks.[62] The companies expected the merger to produce about $1.7 billion in annual cost synergies.[63]

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.[64] The White House release calls these conditions "robust and far-reaching agreements designed to ensure the protection of our national security."[65]

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 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*."[66] 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

62. Alcatel/Lucent Announcement, *supra* note 23, at 2.

63. *Id.* at 3.

64. Press Release, White House, Statement on CFIUS Recommendation Regarding Proposed Merger of Lucent Technologies, Inc., and Alcatel (Nov. 17, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/11/20061117-13.html [hereinafter White House Release]; *see also* Stephanie Kirchgaessner, *Washington Slaps Review on Nokia-Siemens Venture*, FIN. TIMES, Jan. 7, 2007, *available at* http://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* Defense Security Service, Special Security Agreement, *available at* https://www.dss.mil/portal/ShowBinary/BEA%20Repository/new_dss_internet/index.html (search for 'Special Security Agreement') (last visited Oct. 21, 2007); Lucent Techs. Inc., Current Report (Form 8-K) (Nov. 17, 2006) [hereinafter Lucent 8-K]; Alcatel-Lucent Press Release, Alcatel-Lucent Announces Independent Subsidiary to Serve the U.S. Federal Government Market (Dec. 1, 2006) (on file with author); *see also infra* Section IV.B.

65. White House Release, *supra* note 64.

66. Lucent 8-K, *supra* note 64 (emphasis added).

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 of Alcatel and Lucent."[67]

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.

a. 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. [68]

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.[69] The technical standards for terminal 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).

---

67. *Id.*

68. Use of the Carterfone Device in Message Toll Telephone Service, *Declaratory Ruling*, 13 F.C.C.2d 420 (1968); *see also* United States v. Am. Tel. & Tel. Co., 524 F. Supp. 1336, 1348 (D.C. Cir. 1981).

69. 47 C.F.R. § 68 (2000); *see also* 2000 Biennial Regulatory Review of Part 68 of the Commission's Rules and Regulations, *Report & Order*, 15 FCC Rcd. 24,944 (2000) [hereinafter Biennial Review]; 2000 Biennial Regulatory Review of Part 68 of the Commission's Rules and Regulations, *Order on Reconsideration*, 17 FCC Rcd. 8440 (2002); FCC, PART 68 FAQS 1 (2007), http://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. These 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.

).

These standards and procedures apply equally to domestic and foreign-manufactured equipment.

In furtherance of this well-established policy, the FCC adopted in 2005 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."[70]

In addition to promoting competition and innovation in the telecom equipment available to customers in the U.S., 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 U.S. or to obtain any component or service from a third party outside the U.S., as long as the resulting equipment satisfies the FCC's standards and processes for not causing technical harm to telecom networks.[71]

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.[72]

---

70. Internet Policy, *supra* note 38, at 14,988.

71. *See* FCC, EQUIPMENT AUTHORIZATION OF TELEPHONE TERMINAL EQUIPMENT 2 (2006), http://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* note 69, 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, *supra* note 60, at 17 ("We are also dependent on international suppliers for some of our components and subassemblies and for assembly of some of our products."); James Hookway, *Vietnam Vies to Get in on Outsourcing*, WALL ST. J., May 29, 2007, at 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 SEC'Y OF DEF. FOR ACQUISITION, TECH., AND LOGISTICS, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON CRITICAL HOMELAND INFRASTRUCTURE PROTECTION 14 (2007), *available at* http://www.acq.osd.mil/dsb/reports/2007-01-Critical_Homeland_Infrastructure_Protection.pdf ("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. (proposed legislation to ensure that infrastructure critical to national security is controlled by U.S. citizens).

72. *See infra* Section I.B.3(b); *infra* Section III.C (U.S.-Korea Free Trade Agreement);

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 U.S. 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 U.S., but for Alcatel's merger with Lucent and the consequential CFIUS review of this transaction.

b. 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.[73]

Larry Irving et al., *Steps Toward a Global Information Infrastructure*, 47 FED. COMM. L.J. 271, 277 (1994) (Larry Irving, former Assistant Sec'y, U.S. Dept. 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.

).

73. *See* Press Release, Office of the U.S. Trade Rep., USTR Issues 2005 "1377" Review of Telecommunications Trade Agreements (Mar. 31, 2005), *available at* http://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); Press Release, Office of the U.S. Trade Rep., U.S. and Korea Resolve Major Trade Dispute in Telecom Sector (Apr. 23, 2004), *available at* http://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); Press Release, Office of the U.S. Trade Rep., U.S. and EU Implement Agreement to Reduce Barriers on Transatlantic Trade of Telecommunications and Electronics Products (Jan. 17, 2001), *available at* http://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

Similarly, the U.S. government encourages competition 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.[74] 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,[75] 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 U.S. 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 the FCC.

c. 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.

---

telecommunications and electronics products by eliminating duplicative product testing requirements); *infra* Section III.C.

74. *See infra* Section I.B.3(c).

75. *See* NAT'L SEC. TELECOMMS. ADVISORY COMM., ISSUE REVIEW: A REVIEW OF ISSUES ADDRESSED THROUGH NSTAC XXIX (2006), http://www.ncs.gov/nstac/reports/2006/NSTAC%20XXIX%20Issue%20Review.pdf; NAT'L SEC. TELECOMMS. ADVISORY COMM., GLOBALIZATION TASK FORCE REPORT (2000), http://www.ncs.gov/nstac/reports/2000/GTF-Final.pdf; National Communications System, National Security Telecommunications Advisory Committee (NSTAC), http://www.ncs.gov/nstac/nstac.html (last visited Oct. 13, 2007); Network Reliability and Interoperability Council, http://www.nric.org (last visited Oct. 13, 2007).

As noted above, the FCC required prior approval for the addition or termination of interstate lines by carriers.[76] Such regulations were replaced by blanket authorizations, allowing carriers to make independent, market-driven decisions on the equipment to deploy, the locations to deploy the equipment, the features and capacities of the equipment, and the equipment suppliers.[77]

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 approaches 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.[78] 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.[79]

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.[80] Also, the FCC has

---

76. *See supra* notes 44-45.

77. Unbundled Access, *supra* note 49 (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).

78. *See* Motion of AT&T Corp. to be Declared Non-Dominant for International Service, *Order*, 11 FCC Rcd. 17,963 (1996); Motion of AT&T Corp. to be Reclassified as a Non-Dominant Carrier, *Order*, 11 FCC Rcd. 3271 (1995); Policy & Rules Concerning Rates for Dominant Carriers, *Report & Order & Second Further Notice of Proposed Rulemaking*, 4 FCC Rcd. 2873 (1989).

79. *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."); Warren G. Lavey, *Innovative Telecommunications Services and the Benefit of the Doubt*, 27 CAL. W. L. REV. 51 (1990); *supra* notes 36, 38.

80. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended in scattered sections of 18 and 47 U.S.C.); 47 U.S.C. § 1002 (obligations of telecommunications carriers with regard to law enforcement assistance capabilities of its equipment, facilities and services); § 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.

adopted rules for carriers to deploy equipment providing connection to, and automatic location of users by, emergency services.[81] 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 enforcement and emergency services capabilities, the conditions in the National Security Agreement only apply to equipment from one foreign-owned supplier.

d. Nondiscrimination among Telecom Equipment Manufacturers

In addition to the regulatory/antitrust attack on the Bell System's equipment interconnection restrictions, the U.S. 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.[82] 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.[83] 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

).

81. IP-Enabled Services, *First Report & Order & Notice of Proposed Rulemaking*, 20 FCC Rcd. 10,245 (2005); Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Report & Order & Second Further Notice of Proposed Rulemaking*, 18 FCC Rcd. 25,340 (2003).

82. FCC Docket 19129, *supra* note 59; Consolidated Application of American Telephone and Telegraph Company and Specified Bell System Companies for Authorization Under Sections 214 and 310(d) of the Communications Act of 1934, *Memorandum Opinion, Order & Authorization*, 96 F.C.C.2d 18, 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.").

83. Divestiture, *supra* note 34, at 190-91; *see* Warren G. Lavey & Dennis W. Carlton, *Economic Goals and Remedies of the AT&T Modified Final Judgment*, 71 GEO. L.J. 1497 (1983).

procurements through several safeguards.[84] 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.

II. 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 that it adopted for foreign acquisitions.

A. 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. The companies claimed several merger benefits including the following: an 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."[85] The expected synergies included cutting about 10,000 jobs.[86] Because the transaction did not involve a foreign acquirer, there was no CFIUS review. The Antitrust Department of the Justice Department closed its investigation

84. 47 U.S.C. §§ 272, 273.

85. AT&T/BS Press Release, *supra* note 4.

86. *See* AT&T INC., AT&T, BELLSOUTH MERGER: SUBSTANTIAL SYNERGY OPPORTUNITIES, STRENGTHENED GROWTH PLATFORMS IN WIRELESS, BUSINESS AND INTEGRATED SERVICES 36 (2006), http://www.sec.gov/Archives/edgar/data/732713/000095012306002593/y18291se425.htm.

of the transaction on October 11, 2006 without requiring divestitures or imposing any condition.[87]

In contrast, the FCC struggled to reach an order accepted by a majority of the commissioners. With one commissioner recused,[88] 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 merger of Verizon and MCI on the same day).[89] 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.

FCC Chairman Kevin Martin made several attempts to bring an order to a vote for the AT&T/BellSouth transaction.[90] 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.[91] After describing the offered conditions

87. Press Release, Dept. of Justice, Statement by Assistant Attorney General Thomas O. Barnett Regarding the Closing of the Investigation of AT&T's Acquisition of BellSouth (Oct. 11, 2006), *available at* http://www.justice.gov/atr/public/press_releases/2006/218904.htm (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).

88. Statement of Comm'r Robert M. McDowell in the *Memorandum Opinion & Order* in the Application for Transfer of Control Filed by AT&T Inc. and BellSouth Corp., WC Dkt. No. 06-74 (Dec. 18, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-269058A1.pdf.

89. SBC Communications Inc. and AT&T Corp. Applications for Approval of Transfer of Control, *Memorandum Opinion & Order*, 20 FCC Rcd. 18,290, app. F (2005) [hereinafter SBC/AT&T Order]; Verizon/MCI Order, *supra* note 46, at app. G.

90. Public Notice, FCC, 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), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-267857A1.pdf; Public Notice, FCC, Open Commission Meeting Scheduled for October 13, 2006, Cancelled (Oct. 13, 2006), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-267891A1.pdf; Letter from Michael J. Copps & Jonathan S. Adelstein, Comm'rs, FCC, to Kevin J. Martin, Chairman, FCC (Oct. 13, 2006), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-267893A1.pdf; Letter from Kevin J. Martin, Chairman, FCC, to Michael J. Copps & Jonathan S. Adelstein, Comm'rs, FCC (Oct. 13, 2006), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-267892A1.pdf; Public Notice, FCC, Deletion of Agenda Item from November 3, 2006, Open Meeting (Nov. 2, 2006), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DOC-268326A1.pdf.

91. Application for Consent to Transfer of Control Filed by AT&T Inc. and BellSouth

(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."[92] Finally, the companies filed a revised offer of conditions on December 28, 2006.[93] The FCC voted on December 29, 2006 to approve the transaction subject to the offered conditions,[94] and the companies closed the merger that day.[95]

Two other pieces of background information on this transaction are helpful. First, the U.S. government was aware that the U.S. telecommunications industry had lost hundreds of thousands of jobs since its peak around March 2001.[96] The most prominent factors appear to be unrelated to 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.[97] Yet, there had been some articles in 2004 on BellSouth's

---

Corporation, *Public Notice*, 21 FCC Rcd. 11,490 (2006).

92. *Id*. at 11,498.

93. Letter from Robert W. Quinn, Jr., Sr. Vice President, AT&T Inc., to Marlene H. Dortch, Sec'y, FCC (Dec. 28, 2006), *available at* http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518716381 [hereinafter Offer of Conditions].

94. FCC Approves Merger of AT&T Inc. and BellSouth Corp. in *Memorandum Opinion & Order* in Application For Consent to Transfer of Control, WC Dkt. No. 06-74, 2006 WL 3847995 (Dec. 29, 2006).

95. AT&T Inc., Current Report (Form 8-K) (Dec. 29, 2006), *available at* http://www.sec.gov/Archives/edgar/data/732717/000095012306015733/y28428e8vk.txt.

96. *See* U.S. Dept. of Labor Bureau of Labor Statistics, Telecommunications, http://www.bls.gov/oco/cg/cgs020.htm ("Employment in the telecommunications industry is expected to decline 7 percent over the 2004-14 period, compared with 14 percent growth for all industries combined.") (last visited Oct. 13, 2007) [hereinafter BLS Telecommunications]; *The Employment Situation: 2004: Hearing Before the Joint Economic Committee*, 109th Cong. 7 (2004) (statement of Kathleen P. Utgoff, Comm'r, Bureau of Labor Statistics) ("Since March 2001, the telecommunications industry has shed 302,000 jobs."); Michael K. Powell, Chairman, FCC, Remarks at the Goldman Sachs Communicopia XI Conference 1 (Oct. 2, 2002), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-226929A1.pdf (nearly 500,000 jobs lost in the telecommunications industry). *But see* sources cited *supra* note 1; *Accessing the Communications Marketplace: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 110th Cong. (2007) (statement of Kevin J. Martin, Chairman, FCC) ("In 2006, . . . job creation in the industry is high. . . .").

97. *See* BLS Telecommunications, *supra* note 96; Financial Turmoil in the Telecommunications Marketplace; Maintaining the Operations of Essential Communications: Hearing Before the S. Comm. on Commerce, Science, and Transportation, 107th Cong. 6-10 (written statement of Michael K. Powell, Chairman, FCC), *available at* http://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

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.[98]

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.[99] 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."[100]

Second, the AT&T/BellSouth merger was approved by public utility commissions in nineteen states.[101] Conditions for approval of this transaction were adopted by some state regulators, including some conditions 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.[102] 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

---

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.

98. *See* E-BUSINESS STRATEGIES, INC., BELLSOUTH CORPORATION – THE TELECOMMUNICATIONS INDUSTRY LOOKS TO OFFSHORE IT (2004), *available at* http://www.ebstrategy.com/downloads/case_studies/Bellsouth.pdf [hereinafter EBS]; Nick Wreden, *Overseas Outsourcing Bites into Telecom; Political Pressure Keeps Jobs Here, But For How Long?*, AMERICA'S NETWORK, Feb. 15, 2004, *available at* http://findarticles.com/p/articles/mi_m0DUJ/is_2004_Feb_15/ai_n6082741.

99. Comments of Communications Workers of America in Application for Consent to Transfer of Control Filed by AT&T Inc. and BellSouth Corp., WC Dkt. No. 06-74, at 1 (June 5, 2006), *available at* http://svartifoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6518358746 [hereinafter CWA Comments].

100. *Id.* at 4.

101. Offer of Conditions, *supra* note 93, at 1.

102. Press Release, Ky. Pub. Serv. Comm'n, PSC Approves BellSouth Merger with AT&T; Merger Will Have No Immediate Effect on Rates (July 25, 2006), *available at* http://psc.ky.gov/agencies/psc/press/072006/0725_r01.pdf.

order adopted by the Louisiana Public Service Commission did not contain any condition related to jobs.[103]

B. 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:

> 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.[104]

Only Democratic Commissioner Copps — not his Democratic colleague or the Republican commissioners — pointed to this condition in his statement on the merger order.[105] 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 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."[106]

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.[107] Second, the FCC found that the merger

---

103. Request for Approval and/or Letter of Non-Opposition to the Indirect Change in Control of Certain Certificated Entities Resulting From the Planner Merger, *Order*, La. PSC Dkt. 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 Telecomms. Facilities Resulting from Agreement and Plan of Merger between AT&T Inc. and BellSouth Corp., *Notice of Proposed Agency Action & Order Approving Indirect Transfer of Control*, Fla. PSC Dkt. No. 060308-TP (June 23, 2006), *available at* http://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).

104. AT&T/BellSouth Order, *supra* note 3, at 5807.

105. Copps Statement, *supra* note 6, at 5833; *see supra* note 6.

106. *See* Press Release, Commc'ns Workers of Am., CWA: AT&T-BellSouth Merger Will Promote Critical Build-Out of High-Speed Networks (Dec. 29, 2006), *available at* http://www.cwa-union.org/news/page.jsp?itemID=28161726.

107. AT&T/BellSouth Order, *supra* note 3, at 5765-66.

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.[108]

C. 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.

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 a 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-generation of communications services in the U.S.[109] Yet, there

---

> 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 enchancing 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.

Id.

108. *Id.* at 5771.

109. *See* Copps Statement, *supra* note 6, at 6; *see also* IEEE-USA, Position Statement on Offshore Outsourcing, http://www.ieeeusa.org/policy/positions/offshoring.html ("IEEE-USA is particularly concerned that offshoring of engineering, computer science and other high tech

is little to support this linkage.

Copps' 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.[110] 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 U.S. 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.[111] 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

---

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.") (last visited Oct. 13, 2007).

110. *See* BellSouth Corp., Amendment to Annual Report (Form 10-K/A), at 3, 4, 6 (Mar. 1, 2006) (BellSouth described increasing competition and price pressures; realigned asset portfolio toward domestic wireless and broadband, with sale of Latin American operations; business strategy includes "providing superior service and [] 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").

111. *See* EBS, *supra* note 98, at 4-5 (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).

the other hand, the company did not agree to such 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.[112] 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.[113]

Although the FCC has found that improved network technologies and service quality can promote national security,[114] 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.[115] 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 U.S.; 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

112. *See* Paul McDougall, *AT&T to Cut Hundreds of U.S. Tech Jobs, Sources Say*, DR. DOBB'S PORTAL, Sep. 28, 2006, http://www.ddj.com/dept/ai/193100354 ("Programmers in India typically earn at least 60% less than their U.S. counterparts. . . . 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.").

113. *See supra* Section I.B.3(b).

114. AT&T/BellSouth Order, *supra* note 3, at 5766; SBC/AT&T Order, *supra* note 89, at 18,385-89; Verizon/MCI Order, *supra* note 46, at 18,531-35.

115. CWA Comments, *supra* note 99, at 3.

regulators in the increasingly global economy.

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.[116] National security is a component of the FCC's public interest determination for domestic as well as cross-border transactions.[117] 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.[118] However, some of the CFIUS measures for foreign-acquired carriers can be viewed as industry best practices and helpful for U.S. law enforcement, whether implemented by a domestic or foreign-owned carrier.[119] These measures potentially include personnel screening, storing traffic and customer records in the U.S., transmitting and controlling domestic traffic in the U.S., 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

---

116. *See* DT, *supra* note 50; Applications of Guam Cellular and Paging, Inc. and DoCoMo Guam Holdings, Inc., *Memorandum Opinion & Order & Declaratory Ruling*, 21 FCC Rcd. 13,580 (2006); Lewis, *supra* note 17, at 467-72.

117. *See* AT&T/BellSouth Order, *supra* note 3, at 5765-66; SBC/AT&T Order, *supra* note 89, at 18,385-86; Verizon/MCI Order, *supra* note 46, at 18,531-33 ("We take considerations of national security extremely seriously, and we find that the merger has the potential to generate benefits arising from more efficient routing and greater redundancy.").

118. *See supra* note 32 and accompanying text.

119. *See supra* note 98 (The repatriation condition highlights the role of foreign workers and operations for U.S.-owned carriers.); *infra* Section IV.C.

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 governments that the U.S. 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 policies of minimizing regulatory burdens.[120] 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.

III. FOREIGN RESPONSES AND CONTEXT

Sections I and II of this Article 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 U.S. continues to pursue commitments by foreign

120. *See generally* Warren G. Lavey, *Responses by the Federal Communications Commission to WorldCom's Accounting Fraud*, 58 FED. COMM. L.J. 613, 674-77 (2006).

governments to open their telecom sector.

A. 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.[121] With the enactment of the CFIUS reform legislation in July 2007, the Bush Administration emphasized the limited scope of the national security reviews, falling far short of economic protectionism.[122] 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."[123] 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

---

121. *See, e.g.*, Letter from John J. Castellani, President, Bus. Roundtable, to Members of the U.S. Congress 2 (Mar. 27, 2006), *available at* http://www.businessroundtable.org/pdf/32706LettertoCongressCFIUSFINAL.pdf (

> 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.

); *see also supra* notes 18-21.

122. FINSA, *supra* note 11. Press Release, U.S. Dept. of the Treasury, Secretary Paulson Statement on Foreign Investment and National Security Act (July 26, 2007), *available at* http://www.treasury.gov/press/releases/hp509.htm (CFIUS reviewed only about 10 percent of foreign direct investments in 2006); Henry Paulson, Sec'y, U.S. Dept. of the Treasury, Remarks at Press Roundtable in Beijing, China (Aug. 1, 2007), *available at* http://www.treasury.gov/press/releases/hp525.htm (

> [T]he President recently signed CFIUS legislation which I believe is a step forward, a better CFIUS bill. It's focused on national security and the relatively few investments that involve national security every year. . . . We welcome foreign investment in the United States from sovereign wealth funds or any direct foreign investment.

).

123. EUROPEAN COMM'N, UNITED STATES BARRIERS TO TRADE AND INVESTMENT: REPORT FOR 2006 14 (2007), *available at* www.trade.ec.europa.eu/doclib/docs/2007/february/tradoc_133290.pdf.

expressed concern about excessive use which could be interpreted to be a disguised form of protectionism."[124]

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."[125]

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.

B. 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.[126] 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.[127]

---

124. *Id.*

125. EUROPEAN COMM'N DIRECTORATE-GENERAL FOR TRADE, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT AND THE ECONOMIC AND SOCIAL COMMITTEE: A STRONGER EU-US PARTNERSHIP AND A MORE OPEN MARKET FOR THE 21ST CENTURY 7 (2005), *available at* http://www.trade.ec.europa.eu/doclib/docs/2005/may/tradoc_123438.pdf.

126. Peter Lichtenbaum & Andrew D. Irwin, *National Security Review of Foreign Investment: Recent Developments Around the World*, INT'L L. NEWS, Winter 2007, at 13, 14 [hereinafter Lichtenbaum & Irwin].

127. *See* William Hawkins, *Business Should Favor a Stronger CFIUS*, DEFENSENEWS.COM May 8, 2006, *at* http://defensenews.com/story.php?F=1760114&C=commentary.

An article in early 2007 identified several major governments that scrutinize proposed significant foreign investments for potential national security impacts. These countries include Canada, France, Germany, the United Kingdom, Russia, China, and India.[128] 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."[129] In one well-publicized matter in 2005, India's Foreign Investment 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.[130] 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.[131] In Canada, the

---

128. *See* Lichtenbaum & Irwin, *supra* note 126, at 13.

129. *Id.*; *see also* Deborah Solomon, *Foreign Investors Face New Hurdles Across the Globe*, WALL ST. J., July 6, 2007, at A1. In a speech on October 9, 2007, Canada's Minister of Industry Jim Prentice stated an intent to screen foreign acquisitions on grounds of national security following the U.S. example:

> [E]ven the U.S. – that bastion of free enterprise – has the means to 'review and block transactions in the name of national security. . . .' In fact the American Foreign Investment and National Security Act protects the United States' national security, critical infrastructure and key technology. Canada asserts no less right. . . . Canada does not have a national security test for foreign investment. . . . [T]hat's an oversight that should be addressed by this government.

Jim Prentice, Can. Minister of Indus., Address Before the Vancouver Board of Trade (Oct. 9, 2007), *available at* http://www.ic.gc.ca/cmb/welcomeic.nsf/cdd9dc973c4bf6bc852564ca006418a0/85256a5d006b97208525736f00568e03!OpenDocument; *see also* Anna Fifield & Song Jung-a, *Seoul Rethinks Foreign Investment Law*, FIN. TIMES, Oct. 22, 2007, *available at* http://www.ft.com/cms/s/0/c27347a0-80c4-11dc-9f14-0000779fd2ac.html ("Like the US and other countries, Korea already restricts investment in defence-related companies. But there are now at least four amendments to the Foreign Investment Promotion Act before the national assembly aimed at offering greater protections to Korean companies.").

130. *See, e.g.*, Indrajit Basu, *Raising the Red Scare in India's Telecom Sector*, ASIA TIMES ONLINE, Nov. 15, 2005, *at* http://www.atimes.com/atimes/South_Asia/GK16Df02.html; John Ribeiro, *Plan From China's Huawei May Be Blocked in India*, COMPUTERWORLD, Aug. 17, 2005, *available at* http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,103990,00.html .

131. 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 supra* note 7; FCC INT'L BUREAU, REPORT ON INTERNATIONAL TELECOMMUNICATIONS MARKETS 2000 UPDATE 3-4 (2001), *available at* http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-01-117A1.pdf.

Telecommunications Act requires that Canadians control and own at least 80 percent of the voting shares of a telecommunications common carrier.[132] 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.[133] Nevertheless, Canada has not changed its foreign ownership restrictions in the telecom sector.

Similarly, in discussing the CFIUS-reform legislation as well as the openness to foreign direct investment and trade, a senior U.S. Treasury official recently pointed to concerns that Japan continues to shelter its communications industries from competition, new entry, and new product introduction.[134]

C. 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."[135] The announcement went on to state as background: "The United States is aggressively working to open markets globally, regionally and bilaterally and to expand American opportunities in overseas markets."[136]

The Business Roundtable urged the U.S. negotiators to identify and remove non-traditional barriers to the Korean market.[137] This report

---

132. ICT Regulation Toolkit, Practice Note: Foreign Ownership in Canada [3.4.2], http://www.ictregulationtoolkit.org/en/PracticeNote.1882.html (last visited Oct. 13, 2007).

133. *Id.* (report found that restrictions on foreign investment in the sector impeded capital investment by new entrants, growth and productivity).

134. Robert M. Kimmitt, Deputy Sec'y, U.S. Dept. of the Treasury, Remarks on Japan and the United States: Indispensable Partners, in Asia and Beyond (April 17, 2007), *available at* http://www.treasury.gov/press/releases/hp356.htm (noting that foreign direct investment inflows over the past decade averaged 1.6 percent of gross domestic product (GDP) for the U.S., but only 0.1 percent of GDP for Japan; "the United States is open to investment from abroad, and we hope Japan will become more open to investment as well").

135. Press Release, Office of the U.S. Trade Rep., United States, South Korea Announce Intention to Negotiate Free Trade Agreement (Feb. 2, 2006), *available at* http://www.ustr.gov/Document_Library/Press_Releases/2006/February/United_States,_South_Korea_Announce_Intention_to_Negotiate_Free_Trade_Agreement.html?ht=.

136. *Id.*

137. *See* BUS. ROUNDTABLE, REAL LIBERALIZATION IN THE U.S.-KOREA FTA: MOVING BEYOND THE TRADITIONAL FTA (2006), *available at*

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.[138]

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) "[e]nsure[] 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) "[i]nclude groundbreaking safeguards on restrictions that regulators can impose on operators' technology choice, particularly in wireless technologies."[139]

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 U.S. and Korea to "ensure that consumers everywhere reap the benefits of a fully competitive global telecommunications environment."[140] Similarly, the Telecommunications Industry Association, representing telecom equipment manufacturers in the U.S., observed that the agreement will "let the people of both nations continue to use the latest in [information and communication technology] ICT products."[141]

In summary, the U.S. Trade Representative continues to pursue open global telecommunications markets. The CFIUS and FCC actions described in Sections I and II of this Article 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

---

http://64.203.97.43/pdf/20060607000korea_paper.pdf.

138. *Id.* at 7.

139. *Free Trade with Korea: Summary of the KORUS FTA*, TRADE FACTS (Office of the U.S. Trade Rep., D.C.), June 2007, *available at* http://www.ustr.gov/assets/Document_Library/Fact_Sheets/2007/asset_upload_file939_11034.pdf; Office of the U.S. Trade Rep., Final – United States – Korea FTA Texts, http://www.ustr.gov/Trade_Agreements/Bilateral/Republic_of_Korea_FTA/Draft_Text/Section_Index.html (last visited Oct. 13, 2007).

140. *Strong Support for the U.S.-Korea (KORUS) Free Trade Agreement*, TRADE FACTS (Office of the U.S. Trade Rep., D.C.), May 24, 2007, *available at* http://www.ustr.gov/assets/Document_Library/Fact_Sheets/2007/asset_upload_file608_11053.pdf.

141. *Id.* at 4.

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.

IV. ADDRESSING NATIONAL SECURITY VULNERABILITIES THROUGH INDUSTRY-WIDE MEASURES

The restrictions described in Sections I and II 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.[142] 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.

A. 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.

142. *See* NATIONAL INFRASTRUCTURE PROTECTION PLAN, *supra* note 32; Press Release, Dep't of Homeland Sec., Remarks by 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* http://www.dhs.gov/xnews/speeches/sp_1179843074582.shtm; Homeland Security Presidential Directive/HSPD-7, 2003 WL 22962448 (Dec. 17, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

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.[143] Congress has taken an 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[144] and the Security and Accountability for Every Port Act of 2006.[145] 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.[146] The program covers merchant mariners and workers with unescorted access to secure areas of vessels and port facilities. It also 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; it is implemented through the U.S. Coast Guard.[147] The plans include the

---

143. *See* JOHN FRITTELLI & JENNIFER E. LAKE, CONG. RESEARCH SERV., TERMINAL OPERATORS AND THEIR ROLE IN U.S. PORT AND MARITIME SECURITY 3-4 (2006), *available at* http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-9273:1 [hereinafter 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 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.

); Leonard C. Gilroy & Adam B. Summers, *Detailing Foreign Management of U.S. Infrastructure*, REASON.ORG, Mar. 15, 2006, http://www.reason.org/privatization/foreign_management_us_infrastructure.shtml [hereinafter Gilroy & Summers].

144. Maritime Transportation Security Act of 2002 § 102(a), 46 U.S.C. §§ 70101-17 (2006).

145. Security and Accountability for Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified in scattered sections of 6, 19, 31, 42, 46, and 47 U.S.C.).

146. *See* 46 U.S.C. § 70105 (2006); Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 72 Fed. Reg. 3492 (Jan. 25, 2007), *available at* http://www.tsa.gov/assets/pdf/1652-AA41_twic_fr.pdf; Transp. Sec. Admin., Transportation Worker Identification Credential (TWIC) Program, http://www.tsa.gov/what_we_do/layers/twic/index.shtm (last visited Oct. 13, 2007).

147. 46 U.S.C. § 70103(c); 33 C.F.R. § 105 (2006).

following: 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:

> 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 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.[148]

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.[149]

Pursuant to the Aviation and Transportation Security Act of 2001,[150] 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

148. CRS Report, *supra* note 143, at 13.

149. Gilroy & Summers, *supra* note 143.

150. Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified as amended in scattered sections of 49 U.S.C.).

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.[151] 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 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.[152] The airport security programs must include: an airport security coordinator; personnel screening and identification; inspections/audits by TSA; descriptions of the secured areas; access control measures; training programs; and record keeping systems.

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.[153] 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,[154] and has approved some foreign minority interests.[155] With the limited foreign ownership interest in this sector, the point of the following description is not the application

151. *See Travel vs. Terrorism: Federal Workforce in Managing Airport Security: Hearing Before the Subcomm. on the Federal Workforce and Agency Organization of the H. Comm. on Government Reform*, 109th Cong. (2006) (statement of Robert Jamison, Deputy Sec'y for Sec. Operations, Transp. Sec. Admin.), *available at* http://www.tsa.gov/press/speeches/asset_summary_multi_image_with_table_0393.shtm.

152. 49 C.F.R. § 1542 (2006).

153. 42 U.S.C. § 2133(d) (2006).

154. Final Standard Review Plan on Foreign Ownership, Control, or Domination, 64 Fed. Reg. 52,355 (Sept. 28, 1999); 10 C.F.R. § 50.38 (2006).

155. *See, e.g.*, U.S. NUCLEAR REGULATORY COMM'N, INDUS. CONSOLIDATION REVIEW WORKING GROUP, INDUSTRY CONSOLIDATION IMPACT REPORT 58-60 (2002); Three Mile Island, Unit No. 1, *Order*, Dkt. No. 50-289 (Apr. 12, 1999); Order Approving Application Regarding Merger of New England Electric System and The National Grid Group PLC, 64 Fed. Reg. 72367-69 (Dec. 27, 1999).

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.[156] 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.[157] 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.[158]

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 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.[159]

4. Financial Institutions

Banks and other financial institutions operating in the U.S. include a wide range of foreign-owned companies as well as diverse U.S. owners.[160] Concerned about the security of customer information

156. All Operating Power Reactor Licensees, 68 Fed. Reg. 24,517 (May 7, 2003).

157. *See Homeland Security: Monitoring Nuclear Power Plant Security: Hearing Before the Subcomm. on National Security, Emerging Threats and International Relations of the H. Comm. on Government Reform*, 108th Cong. (2004) (statement of Luis A. Reyes, Exec. Dir. for Operations, Nuclear Regulatory Comm'n), *available at* http://www.nrc.gov/reading-rm/doc-collections/congress-docs/congress-testimony/2004/9-14-04-final.pdf.

158. *Id.*; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, NUCLEAR POWER PLANTS: EFFORTS MADE TO UPGRADE SECURITY, BUT THE NUCLEAR REGULATORY COMMISSION'S DESIGN BASIS THREAT PROCESS SHOULD BE IMPROVED (2006), *available at* http://www.gao.gov/new.items/d06388.pdf.

159. Energy Policy Act of 2005 §§ 652-56, Pub. L. No. 109-58, 119 Stat. 594, 810-14 (codified as amended in scattered sections of 42 U.S.C.); *see* U.S. NUCLEAR REGULATORY COMM'N, OFFICE OF NUCLEAR REACTOR REGULATION, ENVIRONMENTAL ASSESSMENT SUPPORTING PROPOSED RULE, POWER REACTOR SECURITY REQUIREMENTS (2006), *available at* http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2006/secy2006-0126/enclosure4.pdf.

160. *See generally* Jose A. Lopez, *Patterns in the Foreign Ownership of U.S. Banking Assets*, Federal Reserve Bank of San Francisco, ECON. LETTER (Fed. Reserve Bank of S.F., Cal.), Nov. 24, 2000, *available at* http://www.frbsf.org/econrsrch/wklyltr/2000/el2000-

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.[161] 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.[162] 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.[163] The five components of 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

35.html.

161. 15 U.S.C. §§ 6801-09 (2006).

162. National security safeguards for financial institutions extend beyond protecting the privacy and security of customers' information to protecting the financial institutions' operations. *See* FIN. SERVS. SECTOR COORDINATING COUNCIL FOR CRITICAL INFRASTRUCTURE PROT. AND HOMELAND SEC., 2006 ANNUAL REPORT (2007), *available at* http://www.fsscc.org/reports/2006/annual_report_2006.pdf.

163. Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002); 16 C.F.R. § 314 (2006); *Protecting Our Nation's Cyberspace: Educational Awareness for the Cyber Citizen: Hearing Before the Subcomm. on Technology, Information Policy, Intergovernmental Relations and the Census of the H. Comm. on Government Reform*, 108th Cong. (2004) (statement of Orson Swindle, Comm'r, Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf; Fed. Trade Comm'n, Financial Institutions and Customer Information: Complying with the Safeguards Rule, http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.shtm (last visited Oct. 13, 2007).

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. The rule does not restrict the storage of customer records to domestic locations. It 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. Last, the Safeguard Rule does not require retention of records for five years.

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

One area of U.S. regulations that imposes additional security restrictions on foreign-owned firms involves contractors and subcontractors performing classified work for the U.S. government.[164] 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 information, including publishing an information systems security policy and appointing an information

164. *See* DEF. TECHNICAL INFO. CTR. (DTIC), DOD 5220.22-M: NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (2006), http://www.dtic.mil/whs/directives/corres/html/522022m.htm (follow pdf hyperlinks).

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.[165]

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.[166] A Special Security Agreement ("SSA") 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. A SSA also 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 transmission, switching, and hosting equipment located only in the U.S., or to store all records in the U.S.; they are not required to screen personnel; and they are not required to retain a neutral third party to perform annual security audits.

---

165. *Id.* at 1-2-1, 2-2-1, 5-1-1, 5-2-1, 6-1-1, 8-1-1, 10-2-1.
166. *Id.* at 2-3-1 to 2-3-5.

C. 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.[167] The communications sector plan ("CS Plan") was developed through broad collaboration by government agencies and industry representatives.[168] The security strategy is aimed at ensuring that "the Nation's communications networks and systems are secure, resilient, and rapidly restored after an incident."[169] 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 "[c]ustomers are responsible for protecting their own assets and access points [as well as] providing for diverse and assured communications to support their specific essential functions."[170]

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 Article, review of the CS Plan will focus on the extent to which this plan applies industry-wide 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

---

167.Press Release, Dep't of Homeland Sec., DHS Completes Key Framework for Critical Infrastructure Protection (May 21, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm; Dep't of Homeland Sec., Fact Sheet: National Infrastructure Protection Program Sector-Specific Plans, http://www.dhs.gov/xnews/gc_1179776352521.shtm (last visited Oct. 13, 2007).

168. COMMUNICATIONS SECTOR PLAN, *supra* note 32, at 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)).

169. *Id.* at 2.

170. *Id.* at 19, 25-26; *see* Letter from Eileen R. Larence, Dir., U.S. Gov. Accountability Office, to Reps. Bennie G. Thompson & Sheila Jackson-Lee, U.S. Cong., at 4 (July 10, 2007), *available at* http://www.gao.gov/new.items/d07706r.pdf (criticizing communications sector plan for failing to "discuss how human assets fit into existing security projects or are relevent to fill the gaps to meet the sector's security goals").

— recommendations for voluntary actions by infrastructure owners and operators "that provide companies with guidance aimed at improving the overall reliability, interoperability and security of networks."[171] 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.

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.[172] 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."[173] 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).[174] These provisions of

171. COMMUNICATIONS SECTOR PLAN, *supra* note 32, at 48, 109 (FCC's Network Reliability and Interoperability Council).

172. *See* Network Reliability and Interoperability Council Best Practices, http://www.bell-labs.com/cgi-user/krauscher/bestp.pl?howDisp=&allrecords=allrecords (last visted Oct. 13, 2007) [hereinafter NRIC].

173. *Id*. at 7-7-5033 (follow '7-7-5033' hyperlink) (last visited Oct. 13, 2007); *see id*. at 7-7-8099 (follow '7-7-8099' hyperlink) (last visited Oct. 13, 2007) ("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.").

174. TELPRI Security Agreement, *supra* note 24, 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 Security Agreement appear to be closer to the Transportation Worker Identification Credential program or the screening for airport employees described above than they are to the applicable voluntary best practices recommendation for the communications industry.[175]

Certain best practices provide recommendations on network routing.[176] However, none of these recommendations even suggests that all companies consider the security benefits of the location restrictions under the Security Agreement, or that all equipment used to transmit, switch, control, manage, or supervise domestic communications be located in the U.S.[177] On the contrary, one of the best practices addresses foreign sites and merely recommends a physical security program for such assets and personnel.[178]

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 U.S. all domestic communications, call records, billing records, and other subscriber information, and retain such information for at least five years.[179] Again, the best practices make several

---

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).

175. *See supra* Section IV.A.1-2.

176. NRIC, *supra* note 172, at 7-7-0520 (follow '7-7-0520' hyperlink) (last visited Oct. 13, 2007) ("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."); *id.* at 7-7-0566 (follow '7-7-0566' hyperlink) (last visited Oct. 13, 2007) ("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)."); *id.* at 7-7-0617 (follow '7-7-0617' hyperlink) (last visited Oct. 13, 2007) ("Network Operators and Service Providers should ensure that routing controls are implemented and managed to prevent adverse routing conditions."); *id.* at 7-7-0731 (follow '7-7-0731' hyperlink) (last visited Oct. 13, 2007) ("Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis."); *id.* at 7-7-1065 (follow '7-7-1065' hyperlink) (last visited Oct. 13, 2007) ("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."); *id.* at 7-7-5105 (follow '7-7-5105' hyperlink) (last visited Oct. 13, 2007) ("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."); *id.* at 7-7-5107 (follow '7-7-5107' hyperlink) (last visited Oct. 13, 2007) ("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.").

177. TELPRI Security Agreement, *supra* note 24, at 7.

178. NRIC, *supra* note 172, at 7-7-5220 (follow '7-7-5220' hyperlink) (last visited Oct. 13, 2007) ("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.").

179. TELPRI Security Agreement, *supra* note 24, at 8-9.

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.[180]

Finally, unlike the Security Agreement's restriction on outsourcing and Commissioner Copps' discussion of the harms of offshore outsourcing,[181] the best practices only address outsourcing in recommending consideration of a quality assessment, functional testing, and security testing by an independent entity.[182]

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 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.

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

180. NRIC, *supra* note 172, at 7-6-1022 (follow '7-7-1022' hyperlink) (last visited Oct. 13, 2007) ("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."); NRIC, *supra* note 172, at 7-7-3217 (follow '7-7-3217' hyperlink) (last visited Oct. 13, 2007) ("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.").

181. TELPRI Security Agreement, *supra* note 24, at 19.

182. NRIC, *supra* note 172, at 7-7-5084 (follow '7-7-5084' hyperlink) (last visited Oct. 13, 2007) ("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.").

> 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.[183]

In the flurry of legislative activity to reform the CFIUS process, leading to the enactment of FINSA in July 2007, legislators, the Bush Administration, business groups, and representatives of labor worked together on assessing the risks and benefits of foreign investments and open markets. However, there has been no legislative or regulatory

183. *Committee on Foreign Investment in the United States (CFIUS), One Year After Dubai Ports World: Hearing Before the H. Comm. on Financial Services*, 110th Cong. 2, 5 (2007) (statement of Clay Lowery, Assistant Sec'y, U.S. Dept. of the Treasury), *available at* http://www.house.gov/apps/list/hearing/financialsvcs_dem/htlowery020707.pdf; *see also* Paulson, *supra* note 16 ("[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.").

effort to level the national security protections from CFIUS reviews across all foreign-owned and U.S.-owned telecommunications companies.[184] Such 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."[185] The signal sent by the National Security Agreement and Special Security Agreement for this transaction 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

---

184. Many of the Security Agreement-type CFIUS conditions date back to 2000 in the agreement covering NTT's acquisition of Verio. Lewis, *supra* note 17, 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 agreement, these conditions do not apply to many foreign-owned service providers and do not apply to domestic-owned service providers. *See Committee on Foreign Investment in the United States (CFIUS), One Year After Dubai Ports World: Hearing Before the H. Comm. on Financial Services*, 110th Cong. 2, 5 (2007) (statement of David Heyman, Dir. of Homeland Sec. Program, Ctr. for Strategic and Int'l Studies), *available at* http://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.

).

185. White House Release, *supra* note 64.

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.[186] Similarly, some regulatory treatments for technically distinct but competing services have converged.[187] 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 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.

186. *See Accessing the Communications Marketplace: Hearing Before the S. Comm. on Commerce, Science and Transportation*, 110th Cong. (2007) (written statement of Kevin J. Martin, Chairman, FCC), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270192A1.pdf.

187. *See, e.g.*, Universal Service Contribution Methodology, *Report & Order & Notice of Proposed Rule Making*, 21 FCC Rcd. 7518 (2006), *review granted in part, vacated in part sub nom.* Vonage Holdings Corp. v. F.C.C., 489 F.3d 1232 (D.C. Cir. 2007) (extending universal service contributions to interconnected voice over Internet Protocol providers is supported by the FCC's principle of competitive neutrality).

MUCH ADO ABOUT NOTHING: THE BIOTECH AND PHARMACEUTICAL INDUSTRIES HAVE LITTLE TO FEAR IN THE POST–*EBAY* WORLD

MICHAEL BEYLKIN*

* Michael Beylkin is a J.D. Candidate at the University of Colorado (2008) and Production Editor of the Journal on Telecommunications and High Technology Law. He will be serving as a judicial clerk for the Honorable Timothy M. Tymkovich on the U.S. Court of Appeals for the Tenth Circuit in Fall 2008. He would like to thank Rebecca Farr, Karam Saab, David Wilson, and Mike Boucher for their comments, suggestions, and help. He would also like to thank Daniela Ronchetti for suggesting the topic for this casenote from the beginning, and for her immense help in the time since in developing and editing the note.

INTRODUCTION

From its humble beginnings, eBay has grown into the dominant leader in the online auction and marketplace arena. eBay offers its buyers, sellers, and visitors an opportunity to browse through millions of product and service offerings, all with the promise of fairness and a truly "free market." Similarly, Thomas Woolston saw the advantages of the Internet and used his creativity and ingenuity to create a method, which he later patented, for building an electronic marketplace.[1] He later assigned this, and other patents, to MercExchange, a company he founded with the hope of commercializing his ideas.[2]

By mid-2000, eBay and MercExchange were both chasing their futures on the Internet. eBay had developed into a formidable force, not only capitalizing on its founder's visions for a "free market" on the Internet, but rapidly growing into one of the most popular and profitable websites on the Internet. MercExchange, on the other hand, was still a fledgling company, having failed to capitalize on its patent portfolio, and it was desperately seeking a foothold in the online auction marketplace. Nevertheless, it would eventually become clear to eBay that it needed to avoid potential patent issues, specifically with respect to those patents held by MercExchange.

Despite several attempts to purchase MercExchange's patent portfolio, eBay failed to reach any workable agreement with MercExchange. Although there is some dispute as to what each of the parties sought out of their proposed arrangement, it is certain that what eBay did next would pave the way for a pivotal 2006 decision in the Supreme Court.

After eBay introduced its "Buy It Now" feature in late 2000 and opened its fixed price website, Half.com, MercExchange, as it has consistently claimed, was left with little choice.[3] In 2001, MercExchange filed suit against eBay, claiming that eBay had infringed on its patents and sought, *inter alia*, a permanent injunction.[4] What would happen over the next five years, from the decision in the district court in Virginia, to the Federal Circuit Court of Appeals, and finally the Supreme Court decision in 2006, would reverberate throughout the patent landscape.

---

1. *See* discussion *infra* Part II.A and notes 42-44.
2. *See* sources cited *infra* note 42.
3. *See* discussion *infra* Part II.A and notes 48-61.
4. *See* Complaint at 16, MercExchange, L.L.C. v. eBay, Inc., No. 2:01-CV-736 (E.D. Va. Nov. 21, 2001).

Prior to the Supreme Court decision in *eBay Inc. v. MercExchange, L.L.C.* ("*eBay*"),[5] an injunction was a matter of course as a remedy after a court had determined infringement had in fact occurred. The Federal Circuit, with rare exception, reversed any attempt to impose a compulsory license as a substitute for an injunction. Its near-automatic injunction rule, although premised on the discretion that a trial court had in determining remedies under the Patent Act, had for all practical purposes, read a "shall" in place of the "may" in Section 283 of the United States Code.[6] The Supreme Court, however, pushed back, and in a unanimous decision, reversed almost three decades of Federal Circuit precedent by mandating an express consideration of the equitable factors that are commensurate with the permanent injunction analysis.

This, as would be expected, created a tremendous amount of confusion among patentees and no more so than in the biotechnology and pharmaceutical industries – industries that rely heavily on patent protection for their financial, research, and market security. Although the distinction between the pharmaceutical and biotechnology industries has blurred in the last decade, there remain some fundamental research and economic distinctions. The differences between the research model of a pharmaceutical company and that of a biotech company may account for a slightly varied approach to patents by each of these industries.[7]

Nevertheless, this casenote argues that the Supreme Court decision will not substantively change the result of the equitable test for injunctive

---

5. eBay, Inc. v. MercExchange, L.L.C., 126 S. Ct. 1837 (2006).

6. *See* 35 U.S.C. § 283 (2000).

7. Pharmaceutical companies are traditionally associated with the prescription drugs and over-the-counter medication used by people around the globe. Large pharmaceutical companies expend billions of dollars on research and development and usually screen millions of compounds in search of a specific effect. This trial and error approach, described by some as "throwing a lot of spaghetti at the wall to see what sticks," has a high failure rate and requires years of financial and intellectual investment. In recent years, pharmaceutical companies have shifted to an investment and sales model. Although they still perform research and development in-house on certain targets and compounds, pharmaceutical companies have begun to invest in drug candidates later in the pipeline, and thereby shift some of the risk to the myriad small and medium-sized biotechnology companies. More and more, pharmaceutical companies are sought out by the biotechnology industry to share in the later development costs and to provide the critical sales force necessary to market the eventual drug and recoup the billions of investment dollars. Biotechnology companies, on the other hand, were initially focused on genetic targets and researched small molecules and proteins with known effects. Advances in genetics, especially in light of the Human Genome Project, spurred an explosion in the number of biotechnology companies. This growth resulted in a concentration of research talent in the biotech sector – which may account for why in recent years, pharmaceutical companies are looking to biotechs as their "research engine." *See generally* Deborah Hopewell, *Biotech vs. Pharma: Once Different, Now Collaborative Entities*, SAN JOSE BUS. J., June 20, 2003, *available at* http://sanjose.bizjournals.com/sanjose/stories/2003/06/23/focus3.html.

relief as it specifically applies to these industries. Further, this casenote addresses each of the four equitable factors and explains how both biotech and pharmaceutical patentees can rely on history and the concurring opinions in *eBay* to remain confident that, with rare exception, they will continue to enjoy the injunctive remedy as a threat against infringement and as a source of investor and marketplace confidence in their innovations.

Part I of this casenote introduces the Patent Act, its history, and its function in incentivizing research and innovation. This incentive is a compromise between a monopoly in the technology for a limited time in exchange for public access to that technology and an eventual dedication of it to the public domain. It also discusses, in general, the requirements for patentability as well as the historical approach of the Federal Circuit to the injunctive remedy for patent infringement.

Part II introduces the dispute between eBay and MercExchange. More importantly, it presents the polar opposite approaches of the District Court of the Eastern District of Virginia and the Federal Circuit Court of Appeals. These decisions highlight the tension that has existed for the previous two decades. Trial courts often placed too much emphasis on individual factors in their equitable analysis prior to granting an injunction. Meanwhile, in practice, the Federal Circuit had adopted a near-automatic rule for granting injunctive relief once infringement had been determined.

Next, Part III reviews the unanimous Supreme Court decision in *eBay*, as well as the two concurring opinions, each of which illustrate the tension of history and the future within the Patent Act and its interpretation by the courts. Additionally, Part III summarizes the arguments presented by eBay, MercExchange, and various amici in their briefs filed with the Supreme Court. While the unanimous opinion clearly requires that trial courts engage the traditional four-factor analysis prior to granting or denying a permanent injunction, the concurring opinions illuminate the considerations that will likely take place in the trial courts' calculus going forward.

Finally in Part IV, this casenote sets forth the reasons for why the biotech and pharmaceutical industries, two key players as amici in the Supreme Court appeal, as well as in the overall patent scheme, have little to fear from the decision. While the promise of an injunction preventing infringment is key to investment and innovation in these industries and the *eBay* decision clearly puts the near-automatic granting of injunctions at risk, this casenote argues that the decision carves out sufficient avenues for trial courts to maintain their historical approach in biotech and pharmaceutical patent infringement cases. This necessarily requires a detailed analysis of the four factors that courts must expressly address and how each of these factors still favor the biotech or pharmaceutical

patentee over a potential infringer. Therefore, this casenote ultimately concludes that while there may truly be an uncertain future to the injunctive remedy in other technological arenas, the biotech and pharmaceutical industries will be largely unaffected by the *eBay* decision and their concern may really be much ado about nothing.

I. INJUNCTIVE RELIEF UNDER THE PATENT ACT AND THE FEDERAL CIRCUIT TEST

A. Patent Act and Injunctive Relief

From the earliest periods of U.S. history, patent law has played an important role in the development of industry and the fostering of a fair and free market in American society. This is mainly due to Congress having near plenary power "[t]o Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[8] Under this grant of authority, patent law and copyright law came into being and have played an integral role in the development and protection of intellectual property rights.

The goal of the United States patent system is to encourage invention and investment into research and development.[9] A patent grants the patentee the "right to exclude others from making, using, offering for sale, or selling [her] invention."[10] Therefore, "[t]he incentive provided by the patent system is a monopolistic rate of return on [the] invention to the patentee."[11] Under such an incentive, inventors are assured that their ideas and novel creations can be protected from the "unscrupulous copyist."[12] Having invested large sums of money and time, this right to exclude is of primary concern to the biotechnology and pharmaceutical industries – where competition is fierce and the value of an invention can be in the hundreds of millions of dollars, if not more.

Three basic requirements must be met in order for an invention to be patentable. First, the invention must be novel or an improvement on something that already exists.[13] This includes a new "process, machine, manufacture, or composition of matter."[14] Because of this novelty requirement, if an invention was known or used by individuals other than

8. U.S. CONST. art. I, § 8.
9. *See* Laitram Corp. v. King Crab, Inc., 244 F. Supp. 9, 14 (D. Alaska 1965).
10. 35 U.S.C. § 154(a)(1).
11. Waterman-Bic Pen Corp. v. W. A. Sheaffer Pen Co., 267 F. Supp. 849, 854 (D. Del. 1967).
12. *See* Graver Tank & Mfg. Co. v. Linde Air Prods., Inc., 339 U.S. 605, 607 (1950).
13. *See* 35 U.S.C. §§ 101-102.
14. 35 U.S.C. § 101.

the patentee, a patent will not issue.[15] Second, the invention must be useful.[16] The utility requirement only demands that some benefit be derived from the invention and that it has some legitimate purpose. Third, the invention must be non-obvious. The test for obviousness is fairly subjective and requires an analysis of whether the invention would have been obvious to one with ordinary skill in the art[17] at the time the invention was developed.[18] Once an invention is patented, the patent holder enjoys certain property rights, such as the right to exclude others from practicing the invention for a limited number of years.

The patent system also provides certain remedies for infringement by others. Generally, anyone who, without authorization, "makes, uses, offers to sell, or sells any patented invention" is liable for infringement.[19] Additionally, anyone who actively induces another party to infringe is also liable.[20] Remedies for infringement include monetary damages as well as permanent injunctions preventing the infringing party from practicing the invention. If infringement is proven in court, damages are statutorily mandated. Section 284 provides that the court "*shall* award . . . damages adequate to compensate for the infringement."[21] Further, increased damages up to three times the amount determined by the court or jury may be proper in some circumstances. Conversely, injunctive relief is not statutorily required in every infringement case. Section 283 provides that "courts . . . *may* grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent" and "*on such terms as the court deems reasonable*."[22] This provision appears to vest considerable discretion in the trial court.[23] Consequently, injunctive relief is not necessarily a guaranteed remedy for a patent holder.

B. The Federal Circuit Approach

The Federal Circuit has recognized that pursuant to 35 U.S.C. § 283, a district court has discretion "to impose a permanent injunction 'in

15. *See* 35 U.S.C. § 102; Metal Arts Co. v. Fuller Co., 389 F.2d 319, 321 (5th Cir. 1968).
16. *See* 35 U.S.C. § 101.
17. Usually, this means skill in the area in which or for which the invention was created. *See* 35 U.S.C. § 103(a). Obviousness is based on factual findings of "(1) the inventor's level of skill in the pertinent art, (2) the scope and content of the prior art, (3) the differences between the prior art and the claimed invention, and (4) secondary considerations." Sun Prods. Group, Inc. v. B&E Sales Co., 700 F. Supp. 366, 375 (E.D. Mich. 1988).
18. *See* 35 U.S.C. § 103(a).
19. 35 U.S.C. § 271(a).
20. *See* 35 U.S.C. § 271(b).
21. 35 U.S.C. § 284 (emphasis added).
22. 35 U.S.C. § 283 (emphasis added).
23. Prior to *eBay*, few district courts successfully exercised such discretion.

accordance with the principles of equity.'"[24]

Further, the Federal Circuit has explained that district courts "enjoy *considerable discretion* in determining whether the facts of a situation require it to issue an injunction."[25] Therefore, the Federal Circuit should review a denial or grant of a permanent injunction under the abuse of discretion standard.[26] But in practice, district court discretion has been significantly limited.

The Supreme Court has stated that a permanent injunction should not issue as a matter of course.[27] In fact, "an injunction should issue only where the intervention of a court of equity 'is essential in order effectually to protect property rights against injuries otherwise irremediable.'"[28] To aid courts in the equitable analysis, the Supreme Court has developed four factors that must be analyzed prior to any determination on permanent injunctive relief.

Under the four-factor test, the plaintiff must show that it has suffered an irreparable injury, that remedies at law are inadequate, that the balance of hardships weighs in its favor, and that the public interest would not be disserved by a permanent injunction.[29] Neither the language of the test, nor the application of these factors outside the patent law landscape typically presumes an injunction once liability has been determined. However, while acknowledging that the traditional principles of equity apply, the Federal Circuit has also stated that, as a general rule, an "injunction will issue when infringement has been adjudged, absent a sound reason for denying it."[30]

The Federal Circuit has used the presumption that a patentee will be irreparably harmed by infringement to justify the granting of an injunction in nearly all cases. Traditional property principles recognize the right to exclude as one of the bundle of rights an owner enjoys.[31] The Federal Circuit has similarly held that the "right to exclude recognized in a patent is but the essence of the concept of property."[32] Therefore, "irreparable harm has been presumed when a clear showing has been

---

24. Odetics, Inc. v. Storage Tech. Corp., 185 F.3d 1259, 1272 (Fed. Cir. 1999) (citing 35 U.S.C. § 283).

25. *Id.* (emphasis added).

26. *Id.*

27. Weinberger v. Romero-Barcelo, 456 U.S. 305, 311 (1982).

28. *Id.* at 312 (quoting Cavanaugh v. Looney, 248 U.S. 453, 456 (1919)).

29. *See id.*

30. Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1247 (Fed. Cir. 1989).

31. *See, e.g.*, Int'l News Serv. v. Assoc. Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) ("An essential element of individual property is the legal right to exclude others from enjoying it. If the property is private, the right of exclusion may be absolute; if the property is affected with a public interest, the right of exclusion is qualified.").

32. *Richardson*, 868 F.2d at 1246-47 (quoting Connel Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548 (Fed. Cir. 1983)).

made of patent validity and infringement."[33]

Only in rare circumstances has the Federal Circuit permitted a finding of infringement and not held that an injunction should necessarily follow. In almost all cases where infringement did not result in an injunction for the patentee, it was because the district court was also required to consider the public interest in the equitable analysis. Consequently, "courts . . . in rare instances [have] exercised their discretion to deny injunctive relief in order to protect the public interest."[34] Typically, the health and safety of the public has been the primary concern in cases where the Federal Circuit has upheld a denial of a permanent injunction after a determination of patent infringement. Such special reasons rarely exist, however.[35] Although there is a "public interest in enforcing valid patents," injunctive relief must have a mechanism for ensuring the availability of critical medical supplies that are integral to the public health.[36] Injunctions may need to be tailored or forgone in circumstances where the public health would be endangered by removal of an infringer's product or service from the market.[37]

Absent these rare exceptions, the Federal Circuit has approached infringement with a near-automatic rule that grants an injunction to the patent holder.

II. THE DISPUTE

A. Background

On Labor Day of 1995, an inconsequential website named AuctionWeb joined three other web pages at a now-popular domain name owned by Pierre Omidyar.[38] Omidyar, a programmer and techie, wanted to create a marketplace that would produce a fair and natural price for goods without discriminating against any type of buyer or seller.[39] Despite his novel concept, seller and buyer traffic did not appear immediately. But, with the help of Usenet groups, web postings, and word-of-mouth across the Internet, AuctionWeb would host thousands of

33. *Id.* at 1247 (quoting H.H. Robertson Co. v. United Steel Deck, Inc., 820 F.2d 384, 390 (Fed. Cir. 1987)).

34. Mallinckrodt, Inc. v. Masimo Corp., 147 F. App'x 158, 177 (Fed. Cir. 2005) (quoting Rite-Hite Corp. v. Kelley Co., 56 F.3d 1538, 1547 (Fed. Cir. 1995)).

35. *See, e.g.*, 35 U.S.C. § 287(c)(1) (exempting medical practitioner's activity that may constitute infringement from the injunctive remedy); Hybritech Inc. v. Abbot Labs., 4 U.S.P.Q.2d (BNA) 1001, 1015 (C.D. Cal. July 14, 1987), *aff'd*, 849 F.2d 1446 (Fed. Cir. 1988); City of Milwaukee v. Activated Sludge, 69 F.2d 577, 593 (7th Cir. 1934).

36. *Hybritech Inc.*, 4 U.S.P.Q.2d (BNA) at 1015.

37. *See City of Milwaukee*, 69 F.2d at 593; *see also* 35 U.S.C. § 287(c)(1).

38. *See* ADAM COHEN, THE PERFECT STORE: INSIDE EBAY 21-22 (2002).

39. *See id.* at 20.

auctions by the end of 1995.[40] On September 1, 1997, the AuctionWeb name was retired, and eBay came to life at www.ebay.com.[41]

Around the end of 1994, an engineer and lawyer named Thomas Woolston was looking for a way to use the Internet to build a business and utilize its advantages in overcoming geographical and communication limitations.[42] He determined that the greatest stumbling block to a marketplace on the Internet was the lack of a medium that could effectively build a web business' trust and reputation.[43] So by April 1995, Woolston filed his first patent application, in what would eventually become part of the family of business-method patents at issue in the litigation with eBay, for a browse-able electronic marketplace.[44] Shortly thereafter, Woolston assigned his patent rights to MercExchange, a company he formed with several business partners.[45]

In December 1998, the United States Patent and Trademark Office ("PTO") issued to MercExchange its first patent, which MercExchange subsequently licensed out within only six weeks.[46] Unfortunately for Woolston, MercExchange did not take off despite numerous attempts to get venture capital funding to commercialize its patents. While Woolston's goal may have been "to build an operating business that would practice his inventions," the economic downturn in the technology market during the dot-com implosion likely ended that proposition.[47] Enter eBay.

Beginning in June 2000, eBay made several attempts to purchase MercExchange's patent portfolio, but met with no success.[48] By this point, eBay had been operating its website for almost five years and was gaining in popularity. MercExchange, on the other hand, was not commercially practicing any of its patents and was looking for relationships with established companies to "capitalize [itself] into an operating company."[49]

The two parties dispute their intentions behind the failed negotiations. eBay contends that MercExchange never intended to sell or license any of its patents, and rather, was using the negotiations as a

---

40. *See id.* at 22-25.

41. *See id.* at 79.

42. *See* Julia Wilkinson, *The eBay Patent Wars: Interview with MercExchange CEO Thomas Woolston*, AUCTIONBYTES.COM, Sept. 30, 2004, http://www.auctionbytes.com/cab/abn/y04/m09/i30/s01; *see also* Brief for Respondent at 1-4, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130).

43. *See* Wilkinson, *supra* note 42.

44. *See* Brief for Respondent, *supra* note 42, at 1-2.

45. *See id.* at 3.

46. *See* Wilkinson, *supra* note 42.

47. *See* Brief for Respondent, *supra* note 42, at 3.

48. *See id.* at 3-4.

49. *Id.* at 3.

ruse to induce infringement.[50] According to eBay, MercExchange, jealous of eBay's success in creating a successful electronic market, had "developed a strategy of suing."[51] MercExchange, however, contends that eBay refused to enter into any extended relationship that would have allowed MercExchange to commercialize its invention. Accordingly, MercExchange argues that eBay chose to willfully infringe on those patents by incorporating MercExchange's technology only several months later. In fall of 2000, eBay introduced a "fixed-price sales capability"[52] that was allegedly encompassed by MercExchange's '265 patent.[53]

MercExchange claims that this infringement, in addition to a lack of capital, prevented it from commercializing its inventions.[54] Consequently, it was forced to build a licensing program as its only means of remaining in business.[55] But this too met with little success. Apparently, one of MercExchange's licensees made payment of royalties contingent on MercExchange preventing further and continued infringement of its patents by eBay.[56]

By 2001, eBay was rapidly becoming the leading online auction marketplace with revenues over $200 million.[57] Half.com had been recently acquired by eBay and was being operated as a wholly-owned subsidiary, offering a fixed-price Internet marketplace.[58] ReturnBuy, a seller of returned retail merchandise, operated a website advertising its goods for sale on eBay's online auction site.[59] Having failed to resurrect its fledgling business through a relationship with eBay, and now apparently stymied in its attempt to license its patents, MercExchange

---

50. *See* Brief of Petitioners at 5-6, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130).

51. *Id.*

52. This is known as the "Buy It Now" feature that is available for certain auctions on eBay's website. *See generally* eBay, http://www.ebay.com (last visited Sept. 29, 2007).

53. Brief for Respondent, *supra* note 42, at 4; *see also* U.S. Patent No. 5,845,265 (filed Nov. 7, 1995).

54. Brief for Respondent, *supra* note 42, at 4.

55. *See id.*

56. *See id.*

57. *See* COHEN, *supra* note 38.

58. *See generally* Half.com, http://www.half.ebay.com/ (last visited Sept. 29, 2007); *see also Company News; eBay to Acquire Half.com, A Trading Site for Used Items*, N.Y. TIMES, June 14, 2000, *available at* http://query.nytimes.com/gst/fullpage.html?res=940DE2DE133EF937A25755C0A9669C8B63.

59. *See* Ina Steiner, *eBay Invests in ReturnBuy Inc.*, AUCTIONBYTES.COM, Apr. 10, 2001, http://www.auctionbytes.com/cab/abn/y01/m04/i10/s03 ("ReturnBuy allows retailers, distributors and manufacturers to reduce processing costs and increase resale revenue on the growing volume of returned merchandise. It uses channels such as eBay to auction returned goods to consumers."); *see also* Bob Tedeschi, *E-Commerce Report; The Success of eBay is Spawning a Number of Online Liquidation Houses*, N.Y. TIMES, Apr. 29, 2002, *available at* http://query.nytimes.com/gst/fullpage.html?res=9B0CE3D91E3EF93AA15757C0A9649C8B63.

sought relief in federal district court.

In September 2001, MercExchange filed suit against the two popular online marketplaces and the seller, claiming patent infringement and seeking a permanent injunction as well as damages.[60] Specifically, MercExchange alleged that eBay, Half.com, and ReturnBuy infringed on three related patents it owned which described an "electronic market" over a "trusted network."[61]

B. District Court Decision

After a five-week trial, which the trial judge described as being "one of the more, if not the most, contentious cases that [his] court [had] ever presided over," the jury found that eBay had willfully infringed two of MercExchange's patents and assessed damages of $35 million.[62] Following the verdict, both MercExchange and eBay filed various post-trial motions, continuing the acrimony that had been such an underlying part of the entire litigation.[63]

The most significant post-trial motion, however, was the MercExchange's Motion for Entry of a Permanent Injunction Order. Under Section 283, once the "infringement and validity of the patents have been established, a district court is authorized to grant a permanent injunction."[64]

Nevertheless, the district court recognized that it had discretion to grant or deny this injunctive relief based on a proper weighing of the traditional equitable factors, which included a consideration of whether MercExchange would suffer irreparable injury without an injunction, whether MercExchange had an adequate remedy at law, whether the public interest weighed in favor of an injunction, and finally whether the balance of hardships are in MercExchange's favor.[65] The court approached each of these factors in turn.

First, MercExchange argued that, without an injunction, it would be deprived of its ability to develop its inventions and thereby, irreparably harmed.[66] Further, it argued that its exclusive right to license these

60. *See* First Amended Complaint, MercExchange, L.L.C. v. eBay Inc., 275 F. Supp. 2d 695 (E.D.Va. 2003) (No. 2:01-CV-736).

61. *See* U.S. Patent No. 6,085,176 (filed Mar. 8 1999); U.S. Patent No. 6,202,051 (filed Feb. 19, 1999); U.S. Patent No. 5,845,265 (filed Nov. 7, 1995).

62. *MercExchange*, 275 F. Supp. 2d at 698-99, 714 (E.D. Va. 2003), *rev'd*, 401 F.3d 1323 (Fed. Cir. 2005), *vacated*, 126 S. Ct. 1837 (2006).

63. *See id.* at 699.

64. *Id.* at 711; *see also* 35 U.S.C. § 283.

65. *See MercExchange*, 275 F. Supp. 2d at 711 (citing factors from *Weinberger*, 456 U.S. at 312).

66. *Id.*

inventions would also be impaired.[67] The district court, however, was receptive to counter-arguments rebutting the presumption of irreparable harm.[68] eBay was able to show that MercExchange (1) had been willing to license its patents, (2) had failed to utilize its patents in commercial activity on its own, and (3) had made comments to the press indicating that it was not seeking an injunction, but merely "appropriate damages" for the infringement.[69] Additionally, the district court pointed out that, although not dispositive, the fact that MercExchange had failed to seek a preliminary injunction weighed against its argument that it would be irreparably harmed.[70] Accordingly, the district court concluded that MercExchange failed to sufficiently establish that it would suffer irreparable harm without a permanent injunction.[71]

Second, MercExchange also failed to show that it lacked an adequate remedy at law. Because it had licensed its patents in the past and had "indicated its willingness to license the patents to the [D]efendants," the court determined that monetary damages could be sufficient and that a compulsory license may be adequate compensation.[72]

Third, in considering the public interest factor, the district court found that it favored neither party. The court recognized that typically the public interest favors the patentee in order to maintain the integrity of the patent system, although there are several notable exceptions. Such exceptions, however, usually exist only when concerns such as public health or gross inequity are implicated.[73] Nevertheless, the court was particularly swayed by eBay's argument that the "growing concern over . . . business-method patents" in both the PTO and Congress indicated that public interest was potentially in their favor.[74] Although the court held that this issue was not dispositive of whether to grant an injunction, it did note that because MercExchange failed to practice its

67. *Id.* As is often argued, MercExchange claimed that the marketplace for its inventions would permit more beneficial terms for a licensing agreement than a court-imposed license. *See id.*

68. *See id.* at 712.

69. *Id.*

70. *See id.*

71. *See id.*

72. *See MercExchange*, 275 F. Supp. 2d at 713. A compulsory license is a "court-imposed license that authorizes the infringer to continue its conduct, presumably upon some payment of monies to the patentee." Mitchell G. Stockwell, *Implementing eBay: New Problems in Guiding Judicial Discretion and Enforcing Patent Rights*, 88 J. PAT. & TRADEMARK OFF. SOC'Y 747, 755 (2006). Compulsory licenses are rare and face significant criticism. *See id.*

73. *See id.*

74. *Id.* at 713-14 (stating that eBay's argument that pending legislation in Congress addressing business-method patents and a new second-level review policy at the PTO was potentially correct and that the public interest may not necessarily be served by an injunction).

business-method patent, the public interest factor was, at least, equalized.[75]

Finally, the court balanced the hardships and determined that a permanent injunction should not issue in this case.[76] It found that any harm to MercExchange, including the possibility of continuing infringement, could be adequately compensated by monetary damages.[77] Further, the court was concerned that an injunction would only breed more contention, impose significant financial costs on both MercExchange and eBay, and expend a considerable amount of judicial resources.[78] In sum, it determined that MercExchange would be fully compensated in the absence of any injunction and denied its Motion for a Permanent Injunction.[79]

C. Federal Circuit Decision

On appeal, the Federal Circuit faced the pertinent issue of whether the district court erred in denying MercExchange a permanent injunction against eBay.[80] It is important to note that the Federal Circuit appeared to address the issue *de novo*, although the proper review had traditionally been under an abuse of discretion standard.[81] In reversing the district court's denial of a permanent injunction, the Federal Circuit dispelled many of the concerns raised under the four-factor equitable test.

As an initial matter, the Federal Circuit identified the typical test for whether to grant an injunction once infringement has been determined. "Because the 'right to exclude recognized in a patent is but the essence of the concept of property,' the general rule is that a permanent injunction *will* issue once infringement and validity have been adjudged."[82] It acknowledged that injunctions have rarely been denied and, in those limited circumstances, usually only in order to protect the public interest.[83]

The Federal Circuit dismissed entirely the conclusions of the district court. First, it held that the district court's concern over business-method patents was misplaced and did not reach the level of an important public need.[84] Second, it found that contentious proceedings and the potential

75. *See id.* at 714.
76. *See id.* at 714-15.
77. *Id.* at 714.
78. *See MercExchange*, 275 F. Supp. 2d at 714.
79. *See id.* at 715.
80. *See MercExchange*, 401 F.3d at 1338.
81. *See* Pierce v. Underwood, 487 U.S. 552, 558 (1988); *Weinberger*, 456 U.S. at 320.
82. *MercExchange*, 401 F.3d at 1338 (quoting *Richardson*, 868 F.2d at 1246-47) (emphasis added).
83. *Id.* at 1338.
84. *Id.* at 1339. The Federal Circuit rejected the district court's concern over business-

for continuing disputes was not only "not unusual" for patent cases, but also would likely occur irrespective of whether an injunction was granted.[85] Third, the Federal Circuit did not agree that MercExchange's willingness to license its patents weighed against an injunction. It held that the "statutory right to exclude is equally available" to both patentees who practice their inventions and those who simply choose to license them.[86] Additionally, the court argued that any leverage a patentee enjoys because of an injunction is a "natural consequence of the right to exclude," and not a consequence that should be avoided by denying an injunction.[87]

Finally, the court held that whether MercExchange had sought a preliminary injunction was inconsequential to the decision of whether to grant a permanent injunction.[88] Consequently, the Federal Circuit held that the district court failed to "provide any persuasive reason . . . [showing] that this case [was] sufficiently exceptional to justify the denial of a permanent injunction."[89]

III. EBAY V. MERCEXCHANGE, 126 S. CT. 1837 (2006)

A little over eight months after the Federal Circuit reinforced its long-held general rule that an "injunction will issue once infringement and validity have been adjudged,"[90] the Supreme Court granted certiorari.[91] eBay's petition for certiorari presented the following question for review by the Supreme Court: "[w]hether the Federal Circuit erred in setting forth a general rule in patent cases that a district court must, absent exceptional circumstances, issue a permanent injunction after a finding of infringement."[92] The Court also requested that the parties address a broader issue: "[w]hether this Court should reconsider its precedents, including *Continental Paper Bag Co. v. Eastern Paper Bag Co.*, 210 U.S. 405 (1908), on when it is appropriate to grant an injunction against a patent infringer."[93]

---

method patents as "not the type of important public need that justifies the unusual step of denying injunctive relief." *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. *See MercExchange*, 401 F.3d at 1339.

89. *Id.*

90. *Richardson*, 868 F.2d at 1246-47.

91. *See* eBay Inc. v. MercExchange, L.L.C., 126 S. Ct. 733 (2005) (granting certiorari to eBay as petitioner).

92. Petition for Writ of Certiorari at i, *eBay Inc.*, 126 S. Ct. 733 (2005) (No. 05-130).

93. *eBay Inc.*, 126 S. Ct. at 733.

A. The Argument Over Equity

The crux of eBay's argument in its appeal to the Court was that the Patent Act mandates that the district court exercise equitable discretion in determining whether a permanent injunction should issue after a finding of patent infringement.[94] Its argument was composed of two basic principles. First, the intent of Congress is clear from the language of the Patent Act where it explicitly vests or limits discretion in the trial court.[95] Second, the Supreme Court does not "interpret a federal statute to require an injunction without regard to equitable principles . . . unless . . . 'textually required.'"[96] Consequently, a district court should grant injunctions "in accordance with the principles of equity"[97] and apply the traditional four-factor test prior to granting a permanent injunction.[98]

eBay argued that the language of the Patent Act vests a varying degree of discretion in the district court to make determinations on the availability of specific remedies for infringement. For example, the court must award damages once it determines that infringement has occurred.[99] This provision vests little discretion other than on the amount of actual damages. Similarly, Section 285 proscribes the awarding of attorney fees in all but "exceptional cases."[100] In contrast, Section 283 places what appears to be broad discretion on the district court with regard to injunctions.[101]

eBay had an unlikely ally in this argument. The United States submitted an amicus brief in support of MercExchange, but nonetheless admitted that Section 283 "confer[s] *discretionary* authority on district courts" and that its plain terms "foreclose any other construction."[102] Even more striking, however, was the government's admission that Section 283 "directs the district courts, when adjudicating private patent rights, to issue injunctions in accordance with the familiar four-factor test."[103] Further, another amicus brief, although neutral with respect to party support, implored that a "rigid rule requiring automatic injunctions in all patent cases absent 'exceptional circumstances' is contrary to the explicit language of 35 U.S.C. § 283 as well as [Supreme Court]

---

94. *See* Brief of Petitioners, *supra* note 50, at 9.

95. *See id.* at 9-10.

96. *Id.* at 18 (citing United States v. Oakland Cannabis Buyers' Coop., 532 U.S. 483, 496 (2001)).

97. 35 U.S.C. § 283.

98. *See* Brief of Petitioners, *supra* note 50, at 11.

99. *See* 35 U.S.C. § 284 (stating that the court "*shall* award the claimant damages adequate to compensate for the infringement" (emphasis added)).

100. 35 U.S.C. § 285.

101. *See* 35 U.S.C. § 283.

102. Brief for the United States as Amicus Curiae Supporting Respondent at 11, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130).

103. *Id.* at 14.

precedent."[104] Consequently, eBay argued that an injunction should not be granted, unless textually required, without consideration of traditional equitable principles.[105] According to eBay, the Federal Circuit, in overturning the district court, had contravened this principle and implemented a "near-automatic" injunction rule.[106]

eBay also found support among the various amici who filed briefs in the appeal to the Supreme Court. An amicus brief submitted by "52 IP Professors" argued that the Federal Circuit, in this decision, as well as in its decisions of the past twenty years, had "abandoned the role of equity" and completely ignored the statutory language of Section 283.[107] Although not completely accurate,[108] they argued that they failed to find even one instance of where the Federal Circuit had permitted a district court to refuse a permanent injunction after a finding of a patent infringement.[109] By failing to apply the equitable factors, the Federal Circuit was allowing some patent owners to perpetrate abuses of the patent system by using the near-automatic injunction standard as a weapon.[110] Patentees with a minimal interest in the infringing product have exacted huge payoffs with the threat of an injunction, usually far in excess of the value of their patent rights.[111] Therefore, the Federal Circuit, by contravening the express language of Section 283, had opened the door to "hold-ups" and inequity in the application of injunctions as a remedy for patent infringement.

Further, eBay argued that *Continental Bag* did not preclude a proper interpretation of Section 283 of the Patent Act and did not act as stare decisis in its case.[112] Chief among its arguments was that a patent holder's "right to exclude," as held in *Continental Bag*, did not address whether an injunction was mandatory in order to protect this right.[113] Further, *Continental Bag* did not address the statutory language of that

---

104. Brief for Teva Pharmaceuticals USA, Inc. as Amicus Curiae in Support of Neither Party at 2, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130) [hereinafter Brief for Teva].

105. *See* Brief of Petitioners, *supra* note 50, at 10-11. eBay cites several circuit court opinions that were overturned where the Supreme Court determined that injunctions should not issue as a matter of course unless the text of the statute requires the court to do so. *See* Amoco Prod. Co. v. Vill. of Gambell, 480 U.S. 531, 544 (1987); *Weinberger*, 456 U.S. at 313; Hecht Co. v. Bowles, 321 U.S. 321, 329 (1944).

106. Brief of Petitioners, *supra* note 50, at 28.

107. Brief for 52 Intellectual Property Professors as Amici Curiae Supporting Petitioners at 1-2, *eBay Inc.*, 126 S. Ct. 1837 (2006) (No. 05-130) [hereinafter Brief for 52 IP Professors].

108. *See* cases cited *supra* note 35.

109. *See id.* at 2.

110. *See id.* at 3.

111. *See id.* at 5-6.

112. *See* Brief of Petitioners, *supra* note 50, at 41-44.

113. *Id.* at 43. This casenote discusses *Continental Bag* in greater detail, *infra*, in Part IV. It held that non-use could not be a consideration in determining whether an injunction should issue. *See Continental Bag Co.*, 210 U.S. at 425-29.

era.[114] And finally, eBay maintained that any language in *Continental Bag* that could be interpreted to remove a district court's equitable discretion was, at most, "non-binding dicta" rather than the substantive holding of the case.[115] As a result, *Continental Bag* did not operate as precedent standing for near-automatic issuance of an injunction and did not preclude the Supreme Court from finding that consideration of the four-factor equitable test was necessary for granting or denying an injunction.

In response, MercExchange tried to walk a fine line, explaining that the Federal Circuit's "general" rule that an injunction should issue upon a finding of infringement was not necessarily synonymous with an "automatic" rule.[116] This "general" approach by the Federal Circuit, according to MercExchange, was more consistent with the underlying purposes of the Patent Act and, despite eBay's contention otherwise, was congruent with traditional equitable principles, supported by historical patent case law, and proper when considering patent policy as a whole.[117]

Although MercExchange recognized that the traditional equitable principles should apply, it also contended that the nature of the rights involved should determine the form of the equitable test.[118] Because the purpose of the Patent Act is to prevent infringement, a "general rule that a particular equitable remedy is necessary to effectuate a congressional purpose" would be "entirely consistent with congressional authorization for courts to exercise equitable powers."[119] Hence, according to MercExchange, there is a presumption of irreparable harm from a violation of the "right to exclude" inherent in patent rights, and an equitable test which grants an injunction "in all but very unusual circumstances" would not be improper.[120]

Similarly, MercExchange argued that the historical purpose of patents has been, and continues to be, to incentivize innovation and sharing of technology, and to promote commercialization of those innovations for the benefit of the public.[121] Such purposes are only served by vigorous enforcement of the right to exclude. In fact, historical practice has been even stricter than the near-automatic rule now followed by the Federal Circuit. Cases from the 19th century

114. *Id.* at 43-44. The language of the controlling patent law of that era was comparable to the current language of 35 U.S.C. § 283. *Compare* Act of Feb. 15, 1819, ch. 19, 3 Stat. 481 *with* 35 U.S.C. § 283.

115. Brief of Petitioners, *supra* note 50, at 44.

116. *See* Brief for Respondent, *supra* note 42, at 15.

117. *See id.*

118. *See id.* at 15-16.

119. *Id.* at 16.

120. *Id.* at 15-16.

121. *Id.* at 20.

typically found an entitlement to an injunction once infringement was proven.[122] Historically, denials of injunctions were rare and were usually based on some exceptional circumstances such as significant financial harm to the defendant or a serious loss of employment with an incommensurately small injury, if any, to the plaintiff patentee.[123]

MercExchange also argued that a near-automatic rule for infringement of patents was not inconsistent with trademark or copyright practice.[124] The comparable trademark remedy provision states that courts "shall have power to grant injunctions, according to the principles of equity and upon such terms as the court may deem reasonable."[125] Similarly, courts "may . . . grant . . . final injunctions on such terms as [they] may deem reasonable" in dealing with copyright infringement.[126] According to MercExchange, the general rule in copyright and trademark cases has been to grant a permanent injunction once past infringement and the potential for future infringement have been proved.[127] Therefore, it was not incongruous for the Federal Circuit to establish a near-automatic injunction rule in patent infringement cases.

Finally, MercExchange argued that only two of the traditional equitable factors are truly at issue in patent infringement. It distinguished *Weinberger* as not offering a four-factor test, but rather focusing on irreparable harm and the inadequacy of legal remedies as the basis for injunctive relief.[128] Accordingly, once infringement has been found, in most cases the plaintiff would have also shown that it lacks an adequate remedy at law.[129] Consequently, without injunctive relief, the plaintiff would not only lack a remedy, but would also suffer a continuing and irreparable harm.

Nevertheless, MercExchange contended that the remaining two factors, even if considered, would almost always favor the patentee. The balance of the hardships would rarely favor the infringing party, except

---

122. *See* Brief for Respondent, *supra* note 42, at 23 n.27.

123. *See id.* at 25 nn.28-29.

124. *See id.* at 26. Part of this argument is based on the underlying purpose of the Federal Circuit which was created, in part, to generate uniformity in intellectual property law.

125. 15 U.S.C. § 1116(a) (2006).

126. 17 U.S.C. § 502(a) (2006).

127. *See* Brief for Respondent, *supra* note 42, at 26.

128. *See id.* at 27 (arguing that *Weinberger*, 456 U.S. at 312, did not create any test for equitable relief).

129. *See id.* at 28. This is similar to a trespass on real property. Damages would be insufficient to recompense for the invasion since the trespasser would not be forced off the land. An injunction, therefore, is the only remedy that compensates for the trespass and prevents future trespass without the necessity for successive lawsuits. *See* Kaiser Aetna v. United States, 444 U.S. 164, 176-79 (1979) (holding that the right to exclude is a fundamental element of the property right); Smith Int'l, Inc. v. Hughes Tool Co., 718 F.2d 1573, 1578 (Fed. Cir. 1983) (holding that the right to exclude would be of much less value without the injunctive remedy).

in unusual circumstances where disproportionate harm would result. However, according to MercExchange, any financial benefits derived from the infringement should not be considered. Similarly, MercExchange argued that "[a]n injunction serves the public interest by protecting the value of patent rights . . . [such as] encouraging the creation, development, disclosure, and commercialization" of new inventions.[130] Following this argument to its logical conclusion, the Federal Circuit's general rule in favor of an injunction in all but extraordinary circumstances was, therefore, entirely consistent with the purpose, language, and historical practice surrounding the Patent Act.

B. Biotech & Pharma Weigh In

Although eBay and MercExchange were the primary parties to the dispute, other important players decided to weigh in through amicus briefs – especially players such as the pharmaceutical and biotechnology industries. The primary concern of the pharmaceutical and biotechnology industries surrounding the *eBay* case and its implications on the injunctive remedy for patent infringement revolves around economics. "The promise of exclusionary rights . . . provides the investment incentive for the research and development of innovative products" that are essential for the public good.[131] The primary asset of most small biotech companies is intellectual property, vis-à-vis patents, and the commensurate right to exclude is essential to justify the high cost and risk of investment.[132] Consequently, an inability to enjoin infringement would diminish economic power and value of patent rights.[133]

As a whole, the biotech industry filed over forty thousand new patents in 2003.[134] However, most of the companies that comprise the biotechnology sector are small and lack significant financial assets. As a result, their primary means of financing research and development is through private investment and negotiations. Consequently, they argued that any change or even uncertainty in the injunctive remedy could have a deleterious effect on negotiations with private investment sources, and thereby reduce the potential for future drug discovery.[135]

Additionally, many biotech companies and research institutions do

---

130. *See* Brief for Respondent, *supra* note 42, at 33.

131. Brief for Biotechnology Industry Organization as Amicus Curiae Supporting Respondent at 1, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130) [hereinafter Brief for BIO].

132. *See id.* at 2; *see also* Brief for Pharmaceutical Research and Manufacturers of America Brief as Amicus Curiae Supporting Respondent at 7, *eBay*, 126 S. Ct. 1837 (2006) (No. 05-130) [hereinafter Brief for Pharma].

133. *See* Brief for BIO, *supra* note 131, at 8.

134. *Id.* at 1.

135. *See id.* at 5.

not immediately practice or develop their patented inventions.[136] In some circumstances this may be due to lack of financing, expertise, or manufacturing capacity. Also, licensing may not be strategically or economically beneficial. If the injunctive remedy was removed as a protection against infringement, the biotech industry would be forced to seek protections under different legal regimes, such as trade secrets, and this may not be in the best interests of the industry or the public as a whole.[137] The rewards of new medicines and improvements to public health and safety may be diminished or lost as a result.

Likewise, the pharmaceutical industry argued that the presumption in favor of a permanent injunction as a remedy for patent infringement is essential. As their amicus brief stated, the "pharmaceutical industry depends for its very existence upon strong, reliable patent protection."[138] The high research and development costs associated with the long process from idea to FDA approval and the high likelihood of failure of most research compounds are subsidized by the products that successfully make it to the drug market.[139] Pharmaceutical drugs usually contain a single, easily identifiable compound that may qualify for patent protection.[140] While an injunction would lead parties to negotiate and reach a fair market price for use, compulsory licensing, as a judicial remedy, rarely factors in the true research and development costs.[141] Therefore, according to the pharmaceutical industry, a failure of the right to exclude in any given circumstance could be disastrous.

Nevertheless, Teva Pharmaceuticals, a generic drug manufacturer, presented a strong counterargument against a near-automatic injunction rule.[142] It argued that injunctions should not issue where the infringement is due to the presence of a "de minimis" or "mere "trifling"

---

136. *See id.* at 17.

137. *See id.* at 9-10. The patent system protects innovation for a limited time in exchange for a dedication of the technology to the public domain at the end of that limited period. *See, e.g.*, Universal Oil Prods. Co. v. Globe Oil & Ref. Co., 322 U.S. 471, 484 (1944). Trade secrets would be a disadvantage to both industry as well as the public. For example, industry would not be protected from reverse engineering or other copying of the technology. *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475-76 (1974). And because trade secrets could, in theory, exist in perpetuity, many innovations may either never make it to market or be limited in supply or distribution, hurting access to it by the general public and limiting the potential innovation on that technology going forward.

138. Brief for Pharma, *supra* note 132, at 5.

139. *See id.* at 5-8.

140. *See id.* at 7.

141. *See id.* at 13-15. Research and development costs of patented drugs are not easily calculable because pharmaceutical companies usually offset the costs of failed drug candidates. *See id.* Consequently, the pharmaceutical industry argued that court-imposed licenses would "directly impact the number of new drugs brought to market. Pharmaceutical companies would be unable to raise as much money to invest in R&D, and the resulting decrease in R&D funding would translate directly into fewer new drugs." *Id.*

142. *See* Brief for Teva, *supra* note 104.

amount of a patented substance in a drug product.[143] According to Teva, because these minute quantities of substances bear little or no significant therapeutic value,[144] an injunction against the entire drug product would be unfair.[145] The patent holder in these scenarios "suffers no competitive disadvantage" and the balancing of the hardships should not weigh in its favor.[146] As one district court stated, it would be a "travesty of equity" to grant an injunction in such cases.[147] A near-automatic rule would thereby restrain generic drug manufacturers and have a concomitant negative impact on the public interest in low-cost pharmaceuticals.[148]

Although it appeared that MercExchange's position enjoyed the support of the biotech and pharmaceutical industry, a strong counter-argument in favor of a full consideration of the four-factor equitable test was nevertheless presented.

C. The Supreme Court

The Supreme Court, in a unanimous opinion, rejected the Federal Circuit's narrow test for an injunction and accepted eBay's argument that the traditional four-factor test applies to injunctive relief under the Patent Act.[149] It held that for an injunction,

> a plaintiff must demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of the hardships between plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.[150]

The Supreme Court found that nothing in the Patent Act indicated a contrary intent by Congress.[151] Neither the language of the statute nor the personal property attributes of patents justified a departure from the traditional balancing test. The use of the term "may" in Section 283 supports this conclusion, as well as the discretion that it vests in the

---

143. *See id.* at 2-3.

144. Typically, these substances are by-products of the chemical or manufacturing processes employed to create the underlying active ingredient. *See id.* at 8-9. Often, eliminating these "impurities" would be cost prohibitive or impossible. *Id.*

145. *See id*.

146. *Id.* at 11 (quoting Abbott Labs. v. Andrx Pharms., Inc., No. 05C1490, 2005 WL 1323435, at *14 (N.D. Ill. June 3, 2005)).

147. *Id.* at 9 (quoting SmithKline Beecham Corp. v. Apotex Corp., 247 F. Supp. 2d 1011, 1045-46 (N.D. Ill. 2003)).

148. *See id.* at 12.

149. *See eBay*, 126 S. Ct. at 1838-39.

150. *Id.* at 1839.

151. *Id.*

district court to perform the requisite inquiry.[152] Also, the existence of a personal property right is separate from any consideration of remedies for violations of that right.[153] Although the Federal Circuit held that the right to exclude, by itself, justified the general rule in favor of a permanent injunction, the Patent Act itself limits this right by making it "[s]ubject to the provisions" of the entire title, including, as the Court found, the remedy provision.[154]

The Supreme Court further supported its decision by comparing the approach to permanent injunctive relief under the Copyright Act, which embodies a similar personal property right and statutory language as the patent statute.[155] Despite numerous attempts by litigants "to replace the traditional equitable considerations" under the Copyright Act, the Supreme Court has "consistently rejected" any rule that would automatically grant an injunction following a determination of copyright infringement.[156]

According to the Court, neither the district court nor the Federal Circuit properly approached the test for injunctive relief. The district court properly identified the four-factor test, but then adopted "expansive principles" that may inequitably deny injunctive relief in certain cases.[157] Specifically, the Court noted that factors, such as a plaintiff's "willingness to license its patents" and a "lack of commercial activity in practicing the patents," could not be conclusive on the issue of whether the patent holder would suffer irreparable harm absent an injunction.[158] On the other hand, the Court determined that the Federal Circuit's decision digressed to the extreme in the opposite direction. Its decision that injunctions should issue in all but exceptional cases was similarly infirm as a categorical rule.[159] However, the opinion offered little guidance on how to apply the equitable principles to the specific facts of the case.

Of particular interest are the two concurring opinions, one by Chief Justice John Roberts and the other by Justice Kennedy. Chief Justice Roberts, joined by Justices Scalia and Ginsburg, concurred with the holding of the Court, but then laid out, at least tacitly, support for the Federal Circuit approach favoring injunctive relief once patent infringement has been determined. He noted that for the last two hundred years, "courts have granted injunctive relief upon a finding of

152. *See id.* (quoting language from 35 U.S.C. § 283).
153. *See id.* at 1840.
154. *Id.* (quoting language from 35 U.S.C. § 261).
155. *See eBay*, 126 S. Ct. at 1840.
156. *Id.*
157. *Id.*
158. *Id.* (quoting *MercExchange*, 275 F. Supp. 2d at 712).
159. *See id.* at 1841.

infringement in the vast majority of patent cases."[160] While he agreed that "[t]his historical practice [did] not *entitle* a patentee to a permanent injunction," he also felt that "'a page of history [was] worth a volume of logic.'"[161]

Justice Kennedy, in his concurring opinion joined by Justices Stevens, Breyer, and Souter, discounted Chief Justice Roberts' attempt to support the Federal Circuit's approach. Of particular importance to Justice Kennedy was the fact that current patent infringement cases are significantly dissimilar from the historical cases that had justified an almost categorical granting of injunctions.[162] In recent years, commercial firms have sprouted up that are dedicated solely to the licensing of patents and not to the manufacturing of goods under the patent protection. Justice Kennedy feared that these firms may use an injunction "as a bargaining tool to charge exorbitant fees to companies that seek to buy licenses to practice the patent[s]" in their collection.[163]

However, Justice Kennedy's most striking conclusion, which has particular importance to the patent law community, was that injunctive relief may not always be in the public interest. According to Justice Kennedy, where the patented method or invention is "but a small component" of the product that an infringing company manufactures, damages may be sufficient compensation to the patent holder.[164] This may be of special concern with respect to business-method patents, which are a recent phenomenon.[165] For these reasons, his call to district courts was to differentiate historical cases from modern incarnations and apply the traditional four-factor analysis on a case-by-case and fact-specific basis.

IV. IMPLICATIONS ON THE BIOTECH AND PHARMACEUTICAL INDUSTRIES

There is definitely confusion as to what the Supreme Court decision in *eBay* actually means to the patent landscape. Given that the clamor for change in patent law has been growing in recent years, largely fueled by "patent trolls" and the use of patents as an offensive tool to exact a ransom, this decision has not been interpreted in a vacuum.[166] Some law

160. *Id.* (Roberts, C.J., concurring).

161. *eBay*, 126 S. Ct. at 1841-42 (Roberts, C.J., concurring) (quoting Justice Holmes in N.Y. Trust Co. v. Eisner, 256 U.S. 345, 349 (1921)).

162. *See id.* at 1842 (Kennedy, J., concurring).

163. *Id.* (Kennedy, J., concurring).

164. *Id.* (Kennedy, J., concurring).

165. *Id.* (Kennedy, J., concurring).

166. *See* Robert A. Armitage, *The Conundrum Confronting Congress: The Patent System Must Be Left Untouched While Being Radically Reformed*, 5 J. MARSHALL REV. INTELL. PROP. L. 268 (2006).

firms are counseling their clients that little, if anything has changed.[167] Others, perhaps, sense a shift from the near-automatic rule that had dominated the Federal Circuit approach for the last twenty years.[168]

Arguably the decision changes very little on its face. The unanimous opinion did little more than reaffirm that traditional equitable principles apply to the analysis of whether to grant injunctive relief. Categorical rules on either side of the argument were expressly renounced by the Court. On one side, the decision states that a failure to commercially exploit or license a patent by a patentee cannot be the grounds for denying a permanent injunction in every case.[169] But that was already the situation under *Continental Bag*.[170] Likewise, a general rule that a permanent injunction should issue once infringement has been determined in every case is antithetical to the specific wording of Section 283 and eliminates the discretion that is statutorily vested in the district court.[171]

The concurring opinions, however, do raise competing issues under the cloak of historical practice. Chief Justice Roberts' opinion, favoring permanent injunctions because of the difficulty in enforcing the "right to exclude," would keep the near-automatic rule in place, at least as an underlying notion in applying the four-factor test.[172] Justice Kennedy would also support a test which favors an injunction, but was careful to point out that many modern patent cases are highly distinguishable from historical ones and such differences need to be addressed in the four-factor analysis.[173]

Nevertheless, the opinion does not necessarily imply that there will be a landmark change in the Federal Circuit analysis, especially for patent disputes in the biotechnology and pharmaceutical industries. One major concern of the industries may lie in whether use or practice of the invention in the marketplace is a dispositive issue on whether a court should grant an injunction for infringement. It is important to note that the core holding of *Continental Bag* was left intact by the Supreme Court

---

167. *See generally* Gregory A. Castanias & Susan M. Gerber, *The Supreme Court's Decision in* eBay*: What Does It Mean for Injunctions in Patent Cases?*, JONES DAY COMMENTARY (June 2006), http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S3507.

168. *See* WILSON SONSINI GOODRICH & ROSATI, CLIENT ALERT: SUPREME COURT ELIMINATES PRESUMPTIVE INJUNCTIONS IN PATENT CASES (2006), http://www.wsgr.com/publications/PDFSearch/clientalert_ebay.pdf; BRYAN C. DINER, ANTHONY C. TRIDICO & JOHN C. STOLPA, FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP, *The Effect of the U.S. Supreme Court's Decision in* eBay v. MercExchange *on the Biopharmaceutical Industry* (2006), http://www.finnegan.com/publications/news-popup.cfm?id=1608&type=article.

169. *See eBay*, 126 S. Ct. at 1840.

170. *See Continental Bag Co.*, 210 U.S. at 425-29.

171. *See eBay*, 126 S. Ct. at 1841.

172. *See id.* (Roberts, C.J., concurring).

173. *See id.* at 1842 (Kennedy, J., concurring).

decision in *eBay*. *Continental Bag*, an almost century-old patent case, stands for the principle that a patent gives the patentee exclusive rights to use of his invention, and that non-use cannot be a factor in determining whether an injunction should issue.[174] *Continental Bag* underscored the core purpose of the patent system was to allow a patentee to "reserve in himself the exclusive use of his invention."[175] If a patentee "neither use[s] his device nor permit[s] others to use it, he has but suppressed his own [rights] . . . [because] he is neither bound to use his discovery himself nor permit others to use it."[176] Consequently, "exclusion may be said to [be] . . . the very essence of the right conferred by the patent, as it is the privilege of any owner of property to use or not use it, without question of motive."[177]

Nevertheless, patent owners who use their invention and compete in the marketplace may have a stronger case for an injunction.[178] This may include manufacturers of drugs or compounds such as pharmaceutical companies, or in the case of some smaller biotechs, licensors of the patent to individual or multiple third parties. The Supreme Court decision does not alter the Federal Circuit framework in such cases.

In contrast, "those who gain no more than negotiating power from an injunction" may have a harder time persuading a court to issue an injunction in addition to, or instead of, money damages.[179] Some patent holders, especially startup biotech and institutional researchers, may have reasons to withhold their invention from the market. Under the post-*eBay* analysis, the more a non-using patent holder resembles a university or individual inventor, the more likely the courts will grant injunctive relief for infringement of the unused invention.[180]

However, it is important to analyze how each of the four factors under the traditional equitable test would balance in a typical pharmaceutical or biotechnology dispute.

A. Irreparable Harm

Prior to the *eBay* case, Federal Circuit precedent presumed irreparable harm to the patentee after infringement was determined.[181]

---

174. *Continental Bag Co.*, 210 U.S. at 425-29.
175. *Id.* at 425.
176. *Id.*
177. *Id.* at 429.
178. *See* Posting of Steven J. Frank to Corporate Dealmaker Forum, Patent Injunctions: Is There Life After eBay v. MercExchange?, http://corporatedealmaker.thedealblogs.com/2006/05/patent_injunctions_is_there_li.php (May 24, 2006) [hereinafter Corporate Dealmaker Forum].
179. *See* Corporate Dealmaker Forum, *supra* note 178.
180. *See id.*
181. *See, e.g.*, *Richardson*, 868 F.2d at 1247.

This, however, was a rebuttable presumption that placed the burden on the infringing party to demonstrate that the patentee would not suffer continuing and irreparable injury absent a permanent injunction.[182] The Supreme Court decision does not address this burden-shift, and this analysis assumes that it remains in place.

Among the several factors that may play a role in deciding whether irreparable injury will result are: whether the patentee uses the invention commercially, whether he licenses the patent to others, and to what degree any irreparable injury has occurred during the pendency of the litigation.[183] While none of these factors may be dispositive on the greater issue of whether an injunction should be granted, each may indicate that any injury sustained may be adequately addressed through another remedy.

However, there are exceptions. Although most pharmaceutical companies and a fair number of biotechnology companies actively commercialize or license their patents,[185] many companies and research institutions, both private and public, do not immediately develop or market their patented products. This may be due to a lack of funding, inadequacy of technology or expertise, or some other roadblock to development.[186] While each of these scenarios could weigh against a finding of an irreparable injury, the unanimous Supreme Court opinion in *eBay* specifically addressed this concern. It recognized that "some patent holders, such as university researchers or self-made inventors, might reasonably prefer to license their patents, rather than undertake efforts to secure the financing necessary to bring their works to market themselves."[187]

Since a patent that is not exploited commercially is more difficult to value than a patent that is licensed or used in the marketplace, biotechnology companies that do fail to practice or license their patents will have a more difficult, but not necessarily impossible, burden. First, they can attempt to prove that the balance of the remaining factors weighs in their favor. While failure to use an invention may weaken the irreparable harm argument, there may still be a significant showing of willful infringement or public harm if an injunction does not issue.

Second, they can choose to license their invention. Nothing

---

182. *See MercExchange*, 401 F.3d at 1339; Reebok Int'l, Ltd. v. J. Baker Inc., 32 F.3d 1552, 1556 (Fed. Cir. 1994) (holding that a showing of infringement raises a rebuttable presumption of irreparable harm in the preliminary injunction context).

183. *See* Polymer Tech., Inc. v. Bridwell, 103 F.3d 970, 974 (Fed. Cir. 1996).

185. *See generally* Brief for BIO, *supra* note 131; Brief for Pharma, *supra* note 132.

186. *See* Brief for BIO, *supra* note 131, at 10-15.

187. *eBay*, 126 S. Ct. at 1840 (stating that "such patent holders may be able to satisfy the traditional four-factor test").

prevents a patentee, such as a small biotech or research institution, from offering the alleged infringer an opportunity to purchase the right to practice the subject matter disclosed in the patent. While this patentee may argue that an injunction can achieve a more favorable, or even more "accurate," fair market value for the patented invention, nothing dictates that the patentee should be able to wield the injunctive remedy as an exploitive tool.[188] Nevertheless, compulsory licenses, as imposed by courts through a damages remedy in place of an injunction, are similarly faulty because they often undervalue the patent or ignore intrinsic elements.[189]

For those inventions that may sit on the proverbial shelf, biotechnology companies can seek protections from other areas of the law, such as trade secrets.[190] In such cases, since the company is choosing to not commercialize or license the invention, it may be of little present benefit to the public, thereby failing to implicate one of the underlying purposes of patent law. Trade secret protection for such innovations would not harm the public and would still offer some protection in the marketplace.

Similarly, the pharmaceutical industry will likely be able to show irreparable injury in the vast majority of infringement cases. Typically, pharmaceutical patents fall into one of two categories. The first category is a basic compound patent. These patents cover the basic compound of a drug, usually the active ingredient, and are often the result of vast expenditures of time and money in research and development.[191] The second category includes subsequent generations of previously expired patents. These patents may cover innovations such as the process involved in manufacturing previously patented ingredients for a drug, new or revised formulations that contain previously patented ingredients, new structural forms of previously patented products, or even impurities in a previously patented ingredient of a drug.[192] Each of these types of patents has a practical commercial use as well as a potential for licensing. Infringement by another company would reduce market share or significantly harm existing licensing agreements and irreparable economic injury would be the likely result absent an injunction.[193]

---

188. *See id.* at 1842 (Kennedy, J., concurring).

189. *See In re* Mahurkar Double Lumen Hemodialysis Cathater Patent Litig., 831 F. Supp. 1354, 1397 (N.D. Ill. 1993), *aff'd*, 71 F.3d 1573 (Fed. Cir. 1995) (holding that "[t]he injunction creates a property right and leads to negotiations between the parties. A private outcome of these negotiations—whether they end in a license at a particular royalty or in the exclusion of an infringer from the market—is much preferable to a judicial guesstimate about what a royalty should be.") [hereinafter *In re Mahurkar*].

190. *See* Brief for BIO, *supra* note 131, at 20.

191. *See* Brief for Pharma, *supra* note 132, at 11-12.

192. *See* Brief for Teva, *supra* note 104, at 12-13.

193. *See* Brief for BIO, *supra* note 131, at 20; Brief for Pharma, *supra* note 132, at 10-

Finally, there may be an additional factor for the patent holder to present in its favor in the irreparable harm analysis. During the usually lengthy process of patent litigation, often lasting several years, there may be either a preliminary injunction in place or otherwise, actual injury may be occurring. The preliminary injunction, although granted on slightly different equitable factors, can serve as a rebuttable presumption that irreparable injury would have occurred, shifting the burden to the infringer.[194] Likewise, if actual injury, such as a loss of market share or a failure of licensing agreements, occurred during the pendency of the litigation, it can serve as almost irrefutable proof that irreparable harm has occurred.

Consequently, the irreparable harm analysis will almost always weigh in favor of a pharmaceutical or biotech patent holder.

B. Lack of a Remedy at Law

With rare exception, a violation of the right to exclude can only be truly rectified with an injunction.[195] This necessarily implies that there is a lack of an adequate remedy at law for patent infringement. Nothing in the Supreme Court opinion in *eBay* likely changes that presumption. While licensing agreements are common throughout the biotechnology and pharmaceutical industries, there is no presumption that willingness to license indicates that money damages may sufficiently compensate for infringement.[196]

The public posture of a company seeking to enforce its patents against an infringing party should play a role in determining whether an injunctive remedy is the sole fair relief. If litigation is merely being used as settlement leverage, then an injunction could provide a windfall to the claimant. Conversely, if the infringement is continuing and a substantial likelihood of a loss of market share or loss of selectivity in licensing agreements exists, then an injunction may be the sole remedy that would compensate for and prevent the harm.

Biotechnology and pharmaceutical companies often license their patent technology to third parties. Willingness to license should not, and according to the *eBay* decision, does not play a role in determining whether an injunction is proper.[197] Nevertheless, licensing agreements in these industries are often carefully written to limit the licensee's use of the patent for specific purposes or to offer exclusive access to the patent for the licensee. Infringement by another party would directly impact

14.

194. *See Reebok Int'l, Ltd.*, 32 F.3d at 1556.
195. *See Kaiser Aetna*, 444 U.S. at 176-79; *Smith Int'l, Inc.*, 718 F.2d at 1578.
196. *See eBay*, 126 S. Ct. at 1840.
197. *See id.*

these contracts and may lessen their value or worse yet, put the licensor-patent holder in breach of contract. An injunction in such cases would be the only remedy that would compensate and secure the patent holder's rights.

Nevertheless, there may be circumstances where infringement, at least in part, may be compensable with money damages and therefore, a remedy at law is available. If a pharmaceutical or biotech company holds a patent to an inactive ingredient that is a miniscule portion of the infringing product, a strong case could be made that damages and a "compulsory license" may be sufficient to remedy the infringement.[198] Likewise, if the patent is to some intermediary compound or process that is not part of the final product, while the infringement may be serious, damages could potentially compensate the patentee sufficiently in circumstances where the public would be harmed by a loss of a competitive marketplace or where the patentee is attempting to prolong its monopoly beyond the initial term. This necessitates a case-by-case analysis and a full exploration by a district court of this equitable factor.

It seems plausible therefore, that these factors will, as they have in the past, usually weigh in favor of the pharmaceutical and biotechnology patentee.

C. Balancing of the Hardships

A balancing of the hardships will almost always favor the patentee against the infringing party. The court must weigh the hardship imposed on the infringing party by an injunction against the patentee's hardship should an injunction be denied.[199] Pharmaceutical and biotechnology research is highly speculative and requires a significant investment of capital, and any diminution in market share or value of an invention because of infringement may impose a tremendous hardship.

Some of the strongest arguments presented by both the pharmaceutical and biotech industries in their amicus briefs were that research costs are often recouped only through the temporary monopoly permitted through the patent system.[200] Such high costs are clear evidence that absent an injunction, a significant, if not debilitating, financial impact would result with continued infringement. It is unlikely that a court could estimate the long-term revenue of a commercially viable drug or other invention and a compulsory license would, only in

198. *See id.* at 1842 (Kennedy, J., concurring) (arguing that legal damages may be sufficient where a patented invention is a small component of a product); Brief for Teva, *supra* note 104, at 14-16.

199. *See eBay*, 126 S. Ct. at 1839.

200. *See* Brief for BIO, *supra* note 131; Brief for Pharma, *supra* note 132.

rare circumstances, successfully incorporate the true market value. [201]

On the other hand, the hardships to the infringing party are usually considered irrespective of the financial impact on the company resulting from it being enjoined from manufacturing the infringing product.[202] While they could argue that a work-around or modification would be cost-prohibitive or infeasible, it is unlikely that such a hardship would outweigh the market damage to the patentee. Loss of employment, bankruptcy, and loss of investor monies would likely result irrespective of which party wins out, and consequently the balancing here is more granular.

However, in circumstances where the infringement is based on a tiny fraction of the drug or invention, such an argument may hold up. With many second and third generation patents, pharmaceutical companies attempt to extend their drug monopolies beyond the initial patent term.[203] Such second and third generation patents are often based on impurities or fractionally present compounds that are not functional in the drug.[204] However, removing such impurities is often cost prohibitive or impossible under currently existing technologies.[205] In such cases, the hardship to the infringing party, such as a generic drug manufacturer, may outweigh the harm that would result from a compulsory license.

On the whole, however, the balance of hardships will usually favor the patent holder. Hence, the post-*eBay* analysis will rarely mandate a different outcome from the near-automatic rule based on this factor alone.

D. Public Interest

The final factor that a district court must consider before granting or denying an injunction is whether the public interest would be disserved by granting an injunction.[206] The near-automatic Federal Circuit rule already incorporated certain aspects of this interest in the "unusual circumstances" exception.[207] The *eBay* decision only requires a closer examination of the effect of a patent monopoly on the general public as well as on any public interest in commercial predictability.

The public interest in the products of pharmaceutical and biotech companies is relatively large. Most pharmaceutical companies create

---

201. *See In re Mahurkar*, 831 F. Supp. at 1397.
202. *See* 1 DAN B. DOBBS, DOBBS LAW OF REMEDIES § 2.4(5) (2d ed. 1993).
203. *See* Brief for Teva, *supra* note 104, at 13.
204. *See id.*
205. *See id.*
206. *See eBay*, 126 S. Ct. at 1839.
207. *See, e.g.*, *Hybritech Inc.*, 4 U.S.P.Q.2d (BNA) at 1015; *Activated Sludge*, 69 F.2d at 593.

drugs that treat illness, prolong life, and improve the health of the general population.[208] Likewise, biotechnology companies often discover the genes that cause cancers, debilitating diseases, and methods for efficacious and safe drug delivery.[209] The patent not only offers the incentive to invest large sums of money into these research endeavors, but also protects the public from products of companies that may seek to provide inferior versions of these innovations.

This factor will almost always favor the patent holder. The amicus briefs of both industries clearly pointed out that absent the patent system's injunctive protections, multi-billion-dollar investment in research and development would likely not be practical.[210] Likewise, if an infringing party is allowed to exact a compulsory license on a regular basis, the investment community would be unable to predict the ultimate value of a drug or innovation, given that on any day, its market share can be depleted without warning.[211]

Nevertheless, there are several circumstances where the public interest would favor the denial of a permanent injunction. First, if the patent is on a drug that was previously protected by a now-expired patent, injunctive relief may be against the public interest.[212] Generic drug companies offer cheaper alternatives to brand-name drugs that have come off patent protection. These lower priced, but usually identical formulations offer the public the opportunity for improved health and quality of life. The patent system was not designed to provide a permanent monopoly to a drug manufacturer and second or third generation patents are often used to perpetuate that stranglehold.

Second, allowing dilute quantities of patented *inactive* ingredients to prevent a generic alternative would likely be deemed against the public interest. Patent law was not meant to permit perpetual exclusive rights in an invention.[213] End-runs around this limitation by a former patent holder could be damaging to the public health, especially because it limits access to medical treatments for lower income individuals. Past cases have carved out public health and safety exceptions to injunctive relief,[214] and such exceptions likely continue to exist after the *eBay* decision.

---

208. *See* Brief for Pharma, *supra* note 132, at 1-2.

209. *See* Brief for BIO, *supra* note 131, at 1-4.

210. *See* Brief for BIO, *supra* note 131; Brief for Pharma, *supra* note 132.

211. *See* Brief for BIO, *supra* note 131, at 3-5; Brief for Pharma, *supra* note 132, at 7-8.

212. *See* Brief for Teva, *supra* note 104, at 9-11.

213. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 150-51 (1989) (stating that the patent system "embodies a . . . bargain for encouraging . . . advances in technology . . . in return for the exclusive right to practice the invention for a *period of years*." (emphasis added)).

214. *See, e.g.*, *Hybritech Inc.*, 4 U.S.P.Q.2d (BNA) at 1015.

Finally, where biotech or pharmaceutical companies have shelved a patented product and thereby prevent the public from access to its benefits, there may be a case for the infringing party.[215] An argument can be put forth that an injunction in such circumstances would remove the drug or innovation entirely from the market, not because of safety or other concerns, but because of a profit motive. A compulsory license in such circumstances may be in the public's interest and may offer strong support to the infringing party in the four-factor analysis.

E. Other Considerations

Nevertheless, even if Justice Kennedy's concurring opinion gains traction in district court analyses, the differences between modern patent cases, such as where business-method patents are involved, and historical cases, which typically include patents held by biotech companies and pharmaceutical companies, should ensure that the near-automatic rule remains in place.

Business-method patents are new phenomena in the marketplace. Prior to the *State Street Bank & Trust*[216] decision, there was an uncertain "business-method" exception to the patentable subject matter under Section 101.[217] Because business-method patents are a more recent evolution in patent law, historical analogues are limited. Therefore, district courts, which may otherwise follow Justice Kennedy's suggestion to use historical practice as guidance in addressing injunctive relief for infringement of business-method patents, may have more latitude under the *eBay* decision to inquire further into the nature of the infringement and its consequences on the market and the parties involved prior to granting an injunction.[218]

Biotech patents and pharmaceutical patents, however, are firmly grounded in historical practice under the patent system. The typical product of both industries is usually a simple compound that is novel, non-obvious, and useful.[219] Historical practice in such scenarios almost exclusively grants an injunction to the patentee, absent exceptional

---

215. *See id.*

216. *See* State St. Bank & Trust Co v. Signature Fin. Group, Inc., 149 F.3d 1368 (Fed. Cir. 1998).

217. *See* Hotel Sec. Checking Co. v. Lorraine Co., 160 F. 467, 469 (2d Cir. 1908) ("A system of transacting business disconnected from the means for carrying out the system is not, within the most liberal interpretation of the term, an art."). *See generally* Automated Financial or Management Data Processing Methods: Business Methods, USPTO White Paper, http://www.uspto.gov/web/menu/busmethp/index.html.

218. This latitude is probably supported by both the opinion of the court in *eBay*, 126 S. Ct. at 1840-41, as well as Justice Kennedy's concurring opinion, *eBay*, 126 S. Ct. at 1842 (Kennedy, J., concurring).

219. *See* Christopher M. Holeman, *Biotechnology's Prescription for Patent Reform*, 5 J. MARSHALL REV. INTELL. PROP. L. 317, 337-38 (2006).

circumstances, and hence the industries' support for the near-automatic rule that had been law prior to *eBay*.

Further, it is unclear whether biotech and pharmaceutical companies will continue to lobby for the near-automatic injunction rule in the future. Biotechnology and pharmaceuticals in the 21st century are becoming more complex. Companies in both sectors increasingly incorporate multiple disciplines in the design and creation of their patentable products, such as biology, chemistry, physics, and engineering, and these novel products are more complex and may require multiple patents.[220] And, it will become increasingly likely that some other player in the market may hold a patent to a fractional component of these complex products. As this trend continues, the industries may become more vulnerable to the threat of an injunctive hold-up.[221] Consequently, they may need to reevaluate their stance on the approach to patent injunctions at some point in the near future.

CONCLUSION

The *eBay* case has signaled the end, at least in principle, to the Federal Circuit's near-automatic injunction rule. On its face, the unanimous opinion merely reaffirmed that traditional equitable principles cannot be overlooked in the permanent injunction analysis. But it offered little, if any, interpretive guidance to the four-factor test.

It is too early to tell if there has been a sea change in patent law and its treatment of permanent injunctive relief after a determination of infringement. The Supreme Court, mindful of institutional competence, left its opinion vague because any substantial change in patent rights was better left for Congressional action. However, in the post-*eBay* era, district courts have reached varying conclusions. Some have incorporated principles from Justice Kennedy's concurring opinion and denied injunctive relief where the infringing technology was but a small part of the overall product and any redesign would have been cost-prohibitive.[222] Others have recited the four-factor test, analyzed the facts of the case, and, nevertheless, applied the equities in favor of a permanent injunction.[223]

Despite the biotechnology and pharmaceutical industries'

---

220. *See id.* at 337-41.

221. *Id.* at 338.

222. *See, e.g.*, z4 Techs., Inc. v. Microsoft Corp., 434 F. Supp. 2d 437, 444 (E.D. Tex. 2006); Paice L.L.C. v. Toyota Motor Corp., No. 2:04-CV-211-DF, 2006 U.S. Dist. LEXIS 61600, at *15-18 (E.D. Tex. Aug. 16, 2006).

223. *See, e.g.*, Visto Corp. v. Seven Networks, Inc., No. 2:03-CV-333-TJW, at *11-14, 2006 U.S. Dist. LEXIS 91453 (E.D. Tex. Dec. 19, 2006); Smith & Nephew, Inc. v. Synthes (U.S.A.), No. 02-2873 Ma/A, 2006 U.S. Dist. LEXIS 91851, at *7-14 (W.D. Tenn. Sept. 28, 2006).

contentions that changing the infringement calculus would have devastating effects on their research and development, investment opportunities, and approach to securing their intellectual property, the *eBay* decision, at least in their case, should not signal a drastic change in their expectations from patent rights. Historically, patent infringement in both industries has been treated by courts with a clear understanding of the ramifications. Courts have typically acknowledged the investor expectations in these industries and that the costly process from a drug lead to an actual marketable pill or treatment necessarily weighs in favor of finding irreparable harm as a consequence of patent infringement. Similarly, monetary damages rarely suffice because it is impossible for courts to accurately predict the long-term value of a pharmaceutical or biotech patent. Because the research is highly speculative, infringement not only diminishes the value of a potential breakthrough, but may short circuit the entire process of drug development, imposing a tremendous hardship on investors and the public alike. And finally, the public interest in the products of both industries, more than in almost any other arena, is exceptionally high. Patents form the foundation for the development of almost every treatment and improvement in public health.

Because the equitable factors weigh heavily in favor of the patentee in the pharmaceutical and biotechnology industries, courts will find it difficult to justify compulsory licensing in place of the traditional permanent injunction. Although the patent future is less clear for business-method patents and "patent trolls," at least in the case of biotech and pharmaceuticals, the *eBay* case is likely much ado about nothing.