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*

Volume subscriptions are available for $45.00. City of Boulder subscribers please add $3.67 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.

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: 4 J. ON TELECOMM. & HIGH TECH. L. __ (2006).

# JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

*Volume 4* *Spring 2006*

# THE UNIVERSITY OF COLORADO SCHOOL OF LAW

## FACULTY, 2005-06

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.

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.

ALLISON HARTWELL EID, *Associate Professor of Law*. A.B., Stanford University; J.D., University of Chicago.

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 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, *Nicholas Rosenbaum 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, *Associate Dean for Research and Professor of Law.* A.B., J.D., University of Illinois.

DAYNA BOWEN MATTHEW, *Associate Dean for Academic Affairs and Associate Professor of Law,* A.B., Harvard-Radcliffe; J.D., University of Virginia.

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.

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

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

MIRANDA PERRY, *Associate Professor of Law.* B.A., Duke University; J.D., University of Chicago; LL.M., New York 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.

KEVIN R. REITZ, *Professor of Law.* B.A., Dartmouth College; J.D., University of Pennsylvania.

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

PIERRE J. SCHLAG, *Byron White Professor of 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, *Associate Professor Emeritus.* B.S., M.D., University of Wisconsin; J.D., University of California, Berkeley.

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

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

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

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

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

PHILIP J. WEISER, *Professor of Law 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.

SIENHO YEE, *Associate Professor of Law.* Peking University, B.A., Brandeis University; J.D., Columbia University; University of Oxford.

### *Research and Clinical Faculty*

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

ROBERT J. DIETER, *Clinical Professor*, *Legal Aid and Defender Program*. B.A., Yale University; J.D., University of Denver.

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.

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.

DONALD L. FORD, *Reference Librarian.* B.A., American University School of International Service; J.D., University of Virginia; M.L.I.S., University of Pittsburgh School of Information Sciences.

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

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

RUSSELL SWEET, *Head of Public Services.* B.A., University of California, Riverside; MAR, Yale University; J.D., University of Washington; M.L., University of Washington.

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.

YVONNE DUTTON, *Legal Writing Professor.* B.A., J.D., Columbia University.

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

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, *2005-06 Silicon Flatirons Fellow Research Associate, Telecommunications.* B.A., University of Kansas; J.D., University of Colorado School of Law.

KRISTIN COLLINS, *Research Fellow, Complex Civil Procedure, Legal Ethics and Professionalism.* B.A., George Washington University; M.Litt., Oxford University; M.A., Columbia University; J.D., Yale Law School.

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.

### *Adjunct, Adjoint and Visiting Faculty*

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

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.

KATHERINE BRIEN, *Senior Attorney, Colorado Office of the Public Defender, Denver, Colorado.* B.A., University of Colorado; J.D., Boston University.

SHARON CAULFIELD, *Attorney at Law, Caplan & Earnest, LLC, Boulder, Colorado.* B.A., J.D., University of Colorado.

CHRISTIE 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.

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

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

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

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

JOHN A. FRANCIS, *Partner, Davis, Graham, & Stubbs, Denver, Colorado.* B.A., University of Colorado; J.D., University of Michigan.

EDWARD J. GAC, *Associate Professor of Taxation and Business Law, College of Business, University of Colorado, Boulder.* A.A., Wright College; B.A., Western Illinois University; J.D., University of Illinois.

CRAIG C. GARBY, *Associate, Gibson, Dunn & Crutcher, LLP, Denver, Colorado.* B.A., University of Colorado; Graduate Research, Waseda University, Tokyo, Japan; M.P.A., Cornell University; J.D., Stanford University.

PHIL GORDON, *Shareholder, Littler Mendelson, P.C., Denver, Colorado.* A.B., Princeton University, J.D., New York University School of Law.

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

NATALIE HANLON-LEH, *Partner, Faegre & Benson, Denver, Co.* B.S., University of Colorado, Boulder; J.D., Harvard University.

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

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

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

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.

CHRISTOPHER D. OZEROFF, *Partner, Hogan & Hartson LLP, Boulder, Colorado.* B.A., Stanford University; J.D., University of Chicago.

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

PATRICK RYAN, *Attorney at Law, P.S.R. Lawfirm, Denver, Colorado.* B.A., M.B.A., Monterey Institute of International Studies; J.D., University of Texas at Austin; M.B.L., Universität St. Gallen, Switzerland; Ph.D. Katholieke Universiteit Leuven, Belgium.

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.

MARK WALTA, *Deputy Public Defender, Colorado Office of the Public Defender, Denver, Colorado.* A.B., Wabash College; M.A., Rutgers University; J.D., Northeastern University.

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

While Volume 4 began with the proceedings of the Silicon Flatirons Telecommunications Program's Fifth Anniversary Symposium, we close with what may be the final chapter on the layered regulatory model debate and a continuation of the communications law reform for the digital age.

This issue begins with a debate on the viability of a layered framework to support communications regulation. David Reed, Chief Strategist of CableLabs, argues against the use of a layered regulatory framework, because it lacks market-based checks and balances, results in a loss of technical neutrality, and stifles innovation.[1] Douglas Sicker, Assistant Professor of Computer Science and Telecommunications at the University of Colorado, counters this argument and insists that the original motivation and design of a layered regulatory model has been misinterpreted. In his article, Professor Sicker argues that a "layered model is still a useful framework for policy making in the current environment."[2]

Recognizing that the pace of technological advancement demands a forward-looking and future-proofing approach to communications regulation, Kyle Dixon, Senior Fellow at Progress & Freedom Foundation, along with Professor Phil Weiser, Associate Professor at the University of Colorado School of Law, proposes an alternative approach that may moot the layered regulatory model debate. In their article, Dixon and Weiser propose various solutions to pressing issues in communications reform, which alter the roles of both federal and state regulators in three broad areas: rate regulation, competition policy adjudication, and consumer fraud.[3]

Paul Teske, Professor of Public Affairs at the University of Colorado at Denver and the Health Sciences Center, comments that the Digital Age Communications Act federal-state framework rightly proposes a more narrowly defined role for state regulation and policy in the future.[4]

---

1. David P. Reed, *Critiquing the Layered Regulatory Model*, 2 J. ON TELECOMM. & HIGH TECH. L. 281.

2. Douglas C. Sicker, *Misunderstanding the Layered Model(s)*, 2. J. ON TELECOMM. & HIGH TECH. L. 299, 301.

3. Kyle Dixon & Philip J. Weiser, *A Digital Age Communications Act Paradigm for Federal-State Relations*, 2. J. ON TELECOM. & HIGH TECH. L. 321.

4. Paul Teske, *Wither the States? Comments on the DACA Federal-State Framework*,

Robert Atkinson, Director of Policy Research at Columbia Institute for Tele-Information (CITI), offers yet another strategy for communications law reform: regulatory gridlock avoidance. Atkinson argues that a fundamental problem facing the telecommunications industry is a gridlocked regulatory process. In his article, he suggests that, given the pace of technological advances, law makers will confront ongoing challenges in their attempts to write "forward-looking" policies and "future-proofed" statutes. The solution, Atkinson argues, is: flexible new statutes that rely on market forces wherever possible, and simple regulatory principles and procedures when necessary as opposed to the gridlock-inducing statutory micromanagement dictated by the 1996 Telecom Act.[5]

We conclude our discussion on digital age communications law reform with an article on privacy and security. Susan Landau, a Distinguished Engineer with Sun Microsystems, argues that the implementation of the Communications Assistance for Law Enforcement Act requirements in Internet networks not only pose risks to the U.S. economy, but also to national security and the freedom of U.S. citizens. Such requirements, she explains, run counter to the U.S. policy trends in the protection of communications privacy begun in the 1970s.[6]

The final article in this issue was the winner of the 2005 Silicon Flatirons Student Writing Competition. Andrew LaFontaine, a JTHTL Comment & Casenote Editor, highlights the concerns and implications of the *SCO v. IBM* copyright and licensing suit on the future of open source development.[7]

This issue was made possible with the contributions from these authors, for which we are most grateful. In addition to the contributions of our eight authors, this issue was published with the tremendous efforts of our staff, the foundation of our Journal's success. In particular, our Articles Editors, Todd Hoy, Eric Lentell, and Alison Minea, worked tirelessly with the authors to develop and publish their articles in this issue, and but for their efforts this issue would not be possible. Additionally, I am awed by our incredibly talented Production Editor, Rita Sanzgiri, and her team of assistants, Jennifer Loyd, Micah Schwalb, and Margot Summers, as their efforts continue to raise the quality of our publication.

---

2 J. ON TELECOM. & HIGH TECH. L. 365.

5. Robert C. Atkinson, *Telecom Regulation for the 21st Century: Avoiding Gridlock, Adapting to Change*, 2 J. ON TELECOMM. & HIGH TECH. L. 379.

6. Susan Landau, *National Security on the Line*, 2 J. ON TELECOMM. & HIGH TECH. L. 409.

7. Andrew LaFontaine, *Adventures in Software Licensing: SCO v. IBM and the Future of the Open Source Model*, 2 J. ON TELECOMM. & HIGH TECH. L. 449.

I am particularly grateful for the 3L members of our staff. As the end of the year and graduation drew nigh, you continued to stay engaged to finish our tasks. I am equally impressed by our 2L members, all of whom have benefited from the able assistance of our fantastic team of Comment & Casenote Editors: Molly Ferrer, Andrew LaFontaine, and Cynthia Sweet—the true Unsung Heroes of our Journal staff. The contributions of our Executive Editor, Zachary Lange, have enabled us to efficiently operate as a team and to ensure that the communications needs of our staff are met; I could not have done it without you. I cannot forget the tremendous efforts of our Managing Editor, Travis Litman; his contributions to both the Journal operations and business management enabled us to increase our subscriptions by thirty percent this year.

Beyond the Journal staff, there are many others who deserve recognition. First, we welcome two new faculty supporters: Brad Bernthal and Professor Paul Ohm. Brad Bernthal, our Silicon Flatirons Fellow Research Associate, supported the introduction of our 2L Scholarship Review Luncheon and mentored and supported our Journal members as participants in the Trademark and Telecommunications National Moot Court competitions. Additionally, we are also grateful that Professor Paul Ohm accepted the challenge to serve as our faculty co-advisor along with Professor Weiser. We look forward to your contributions to the Journal and recognize the gift that we have been given in your mentorship. Second, we cannot find words to express our gratitude for the Silicon Flatiron Telecommunications Program and JTHTL Board. Your continued support allows our Journal to reach new heights; thank you.

Finally, we are humbled by the commitment to student development that Professor Phil Weiser has continued to demonstrate throughout this past year. We are blessed to have such an exceptionally talented and caring advisor. We cannot thank you enough for your personal touch—you meet us where we need you and deliver every time. You epitomize the professor, counselor, mentor, and friend that all should seek in an advisor; you make us want to learn and do more. Thank you!

These expressions serve as a token of our gratitude for those who support our efforts. As such, it is with great pleasure that we publish Volume 4, Issue 2 of the *Journal on Telecommunications and High Technology Law*. We are certain that this issue will continue to feed your intellectual curiosity in telecommunications and technology law and policy.

*Lisa M. Neal-Graves*
*Editor-in-Chief*

# JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

*Volume 4* *Spring 2006*

## CONTENTS

### THE LAYERED REGULATORY MODEL DEBATE



### DIGITAL AGE COMMUNICATIONS LAW REFORM



### SILICON FLATIRONS STUDENT WRITING CONTEST 2005

# CRITIQUING THE LAYERED REGULATORY MODEL

DAVID P. REED*



## INTRODUCTION

Today there is considerable debate regarding the application of a "layered model for regulation" of telecommunications services.[1] A layered regulatory model establishes a set of layers, each with its own set of permitted functions, to serve as a guide to regulatory decision-making. Roughly speaking, most of the proposed frameworks include four layers: 1) a physical network layer, 2) a logical network layer, 3) an application layer, and 4) a content layer. An examination of several specific

* Executive V.P. and Chief Strategy Officer, CableLabs. Before working at CableLabs, Dr. Reed served for three years at the Federal Communications Commission as a Telecommunications Policy Analyst in the Office of Plans and Policy. The author's views expressed in this article are not representative of CableLabs. The author extends his thanks and gratitude for the able assistance of Travis E. Litman, a CableLabs intern, University of Colorado School of Law student, and Managing Editor of the JTHTL.

1. *See* Douglas C. Sicker & Joshua L. Mindel, *Refinements of a Layered Model for Telecommunications Policy*, 1 J. ON TELECOMM. & HIGH TECH. L. 69 (2002); Adam Thierer, *Are 'Dumb Pipe' Mandates Smart Public Policy? Vertical Integration, Net Neutrality, and the Network Layers Model*, 3 J. ON TELECOMM. & HIGH TECH. L. 275 (2005); Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. ON TELECOMM. & HIGH TECH. L. 37 (2002); Richard S. Whitt, *A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587 (2004).

proposals in this regard falls beyond the scope of this paper.[2] Instead, this article offers a critique of the general idea of applying a layered regulatory framework on communications services in the United States.

My critique of the layered model follows an interdisciplinary approach with concerns organized along economic, technical, and public policy grounds. Specifically, when applied to specifications developed by CableLabs for various IP-enabled offerings, the layered model presents a poor paradigm by which to pursue regulation.

This article argues that regulations which impose access requirements based upon a layered engineering framework lack market-based checks and balances, result in a loss of technical neutrality, and stifle innovation. The article begins by looking at a set of economic failings that arise in the context of layered regulation. Specifically, under close examination, the layered model is little more than a veiled attempt to unbundle the network by imposing open access requirements on facilities-based carriers. In the past, similar regulatory unbundling efforts met with uneven success due to the inherent complexity of pricing unbundled components in a public forum, the strident gaming of all participants in the regulatory process, and the lack of market pricing of unbundled elements.

Part II of the article focuses on how the current broadband cable networks are designed with regard to protocol layers associated with a layered regulatory model. This technical analysis is described in the context of the network platforms designed and developed at CableLabs. The risk presented by imposing regulation on CableLabs specifications highlights the threats to technical neutrality. In other words, implementation of a layered model will place regulators in the position of selecting technical winners and losers, instead of relying upon the market, since regulations defining the layer interfaces must publish the specific technical elements to be maintained across layers. This means a loss of technical neutrality in regulation as specific technical implementations are ratified. In turn, a lesson of warning can be gleaned from looking at CableLabs as a model for other network platforms such as those designed for telephone and mobile phone networks.

Finally, Part III describes how the application of the layered model for regulation would result in poor public policy. In reality, network systems and public policy do not intersect in the clean, simple fashion

2. For an overview, *see* Philip J. Weiser, *Toward a Next Generation Regulatory Strategy*, 35 LOY. U. CHI. L.J. 41 (2003); *see also* Douglas C. Sicker, *Misunderstanding the Layers Model*, 4 J. ON TELECOMM. & HIGH TECH. L. 299 (2006). Suffice to say that most proposals do not agree on the exact definition for the set of layers that would serve as the best regulatory model. This fact in itself – that advocates cannot immediately agree on the precise definition of the layers – provides telling commentary as to the considerable complexity of a layered regulatory model.

that advocates of the layered model portray. The layered model presupposes the current layered structure of network systems, namely those based upon the Internet, will remain relatively stable in the foreseeable future. This may or may not be true. Moreover, strong interdependencies exist today between technical layers. A layered regulatory model would require technical changes to the current network platforms to meet its new requirements, and is certain to influence the path of future development of the network platforms. As such, regulators will become key decision-makers in approving the path of network evolution as it maps to their layered model, and could stifle innovation in cross-layer network technologies through this regulatory control.

## I. ECONOMIC CONCERNS

The economic concerns that arise from a layered regulatory model should underpin any dialogue between regulators, public policymakers, and industry. The layered approach may be seen as a framework for unbundling which involves questions of market access and pricing inasmuch as it is about "network layers." As a result, it is vital that both regulators and industry participants recognize the potential economic consequences which inhere in a layered system.

A major thrust behind the impulse toward a layered model is the application of a consistent regulatory framework to service providers based upon the specific layer functionalities they provide, rather than the historical regulatory precedent of their industry.[3] Once the layers are determined, regulatory rules would govern how service providers could provide both specific layer services as well as cross-layer services for multi-layer functionalities. In terms of economic regulation, the restrictions placed upon any provider in offering services to a particular layer, or across multiple layers, would be determined by its market power where established by the layered services. A service provider would thus be precluded from leveraging substantial market power in one layer to establish a dominant market position in another layer through vertical integration of services up (or down) through the layered stack.

The attractiveness of the layered model, therefore, is that it represents a means for organizing different categories of network functionalities for the purposes of economic regulation. More specifically, it provides a model through which regulators can implement a horizontal segmentation of the markets as represented by each layer (while still preserving the vertical-layer network interoperability required for telecommunications services). In other words, this is simply a

3. *See* Werbach, *supra* note 1, at 59.

mechanism to implement *logical unbundling* of network elements by another name.[4] What is different here is that the layered model of engineers provides the construct for identifying the functional element categories and the interfaces required across each layer boundary, rather than a model developed by policy makers.

Historically, logical unbundling models such as *Computer Inquiries I – III* and *Video Dialtone* were pursued in the presence of market power as a means to ensure network access to achieve economic benefits associated with open competition.[5] Regulators are likely to encounter technical difficulties (as explained by the CableLabs case study below) in trying to cleanly separate and associate specific layers with the services of a particular service provider.

From an economic perspective, an equally notable concern of regulatory unbundling regimes is how the unbundled elements are priced, since price is the ultimate arbiter of network access. Incumbents with market power are incented to overprice unbundled elements to discourage new entry, while new entrants have incentives to discount unbundled elements that provide them a subsidy to establish themselves as a new service provider. As a result, regulators are stuck in the middle trying to somehow discern what only the invisible hand of the market can ultimately decide. Because of this basic tension, unbundled network elements have become a costly source of conflict and litigation.[6]

Implementation of a layered regulatory model would encounter just these problems. At the outset, assuming that the layer boundaries can even be defined, allegations of unfair pricing of layered services will inevitably be brought to the regulatory authorities wherever it may serve a business interest. In turn, regulators will be placed in the position of having to decide whether or not the service layer pricing is fair. This is precisely the role and type of decision-making that regulators are notoriously poor at due both to public choice pressures and the law of unintended consequences. In other words, because regulators have no divine insights into the efficient setting of market prices for complex

4. Here, the term logical applies not to the logical network layer, but to the notion of unbundling the software elements of a network from other hardware and software elements of the network.

5. Nat'l Cable Television Ass'n. v. FCC, 33 F.3d 66 (D.C. Cir. 1994) [hereinafter *Video Dialtone*]; Regulatory and Policy Problems Presented by the Interdependence of Computer and Communications Services and Facilities, *Notice of Inquiry*, 7 F.C.C.2d 11 (1966) [hereinafter *Computer Inquiry*]; Amendment of Section 64.702 of the Commission's Rules and Regulations, *Final Decision*, 77 F.C.C.2d 384 (1980) [hereinafter *Second Computer Inquiry*]; Amendment to Sections 64.702 of the Commission's Rules and Regulations, *Memorandum Opinion & Order on Reconsideration*, 3 FCC Rcd. 1150 (1988) [hereinafter *Third Computer Inquiry*].

6. *See, e.g.,* United States Telecom Ass'n v. FCC, 359 F.3d 554 (D.C. Cir. 2004); United States Telecom Ass'n v. FCC, 290 F.3d 415 (D.C. Cir. 2002).

services, they are an ineffective proxy for market-based decisions.

In short, the layered regulatory model is really just another attempt at network unbundling, and therefore suffers from the same fatal flaws of previously proposed or implemented network unbundling regulatory regimes. The key to unbundling is the pricing of the unbundled network elements. Unfortunately, mandatory unbundling to meet regulation means that regulators, not market mechanisms, are setting the prices of unbundled elements. Regulators are ill equipped to serve this role. The heavy hand of regulation in the form of the layered model represents a highly invasive regulatory model. This model places less reliance on market mechanisms than other possible regulatory models (such as the promotion and establishment of facilities-based competition) and should be disfavored.

Unbundling through the mandatory establishment of network layers can reduce network efficiency by precluding the realization of economies of scale, scope, or other material benefits across the unbundled interfaces. The embedded implementations in the PacketCable Multimedia Terminal Adapter (MTA) and CableHome Residential Gateway (RG) as described in Part II are tangible examples of how this can translate into economic concerns. Without the ability to deploy an embedded interface with cross-layered functionality, the ability to add devices to the network would require interface development for each new device, thereby increasing the deployment cost and time. Cable operators would suffer a much longer device deployment time in the market since it would take longer to specify the protocols needed to support a standalone MTA and a higher device cost since it would demand a higher level of complexity in the new protocols to support the interface. Thus, the ultimate calculus for a layered model actually promotes lost efficiency.

If few economies of scale and scope exist across the network and application layers, then a layered approach can be an efficient technical solution. Again, however, to the extent that market mechanisms are left in place, such a regime would better promote a successful implementation. The PacketCable Multimedia specification described in Part II is an example of an approach that more easily conforms to a layered description. The important point here is that cable operators – unsure of what the ultimate economic equation will be – have developed both the PacketCable VoIP specification, a more fully specified architecture with cross-layer functionalities, and PacketCable Multimedia, a more generic layered architecture. Cable operators will use their experiences in the market to determine their ultimate path of service deployment, and the technical platform that best fits each of their own individual deployment strategies. However, the introduction of regulation here gives cause for concern because a layered regulatory

model presupposes one specific architectural approach. Indeed, any time that regulators can or should decide a specific technical architecture for the market yields cause for concern for the reasons outlined above.

A further concern is that innovation may be stifled by any assertion of regulatory control. Regulatory oversight and approval processes will hinder deployment and development of new capabilities and services based on cross-layer technologies. Once any particular interface is adopted and approved, the combination of regulatory inertia and the interest of industry incumbents will make it difficult for new technologies or techniques to be introduced. Additionally, regulatory precedent will direct investment in technologies, again influencing the direction and pace of innovation. All these actions will increase development costs, and introduce potentially inefficient market dynamics into the process of innovation.

A final economic concern is the simple observation that the economic interests of service providers along each layer, and across different layers, often will not be aligned.[7] This intrinsic element of the layered model means that controversy will be endemic to its regulatory application if firms are restricted to offering services in specific layers, or access to a particular layer must be provided to firms offering different layer services. In turn, logical outflows like protocol wars and regulatory gaming may become commonplace.

One way to change the impact of regulation in a layered model will be to change the protocols capabilities. Protocols are dynamic specifications that change over time to refine or include new capabilities. With the intense scrutiny on the technical capabilities incorporated into each protocol at each layer, one can imagine "protocol wars" will erupt as functionalities are placed at different layers to ameliorate or exacerbate the impact of regulatory decisions. These protocol wars may in fact undercut the whole basis of imposing a layered model, particularly as new technologies with destructive capabilities are introduced. Finally, a layered model must account for the presence of a large number of essential, cross-layer functionalities as will be described in Part II. Clearly, the scope and implementation of such cross-layer services will be a lightning rod for regulatory controversy under this paradigm. Inevitably, cross-layer services will often have to be approved by regulators, and it will be in the economic interest for firms competing at another layer to try to use these proceedings to constrain competition in their layer by either eliminating or severely constraining the scope of permitted capabilities. Given the disparate economic interests at hand, regulators will be placed in the middle to resolve complex technical and

7. For further discussion and support of this observation, *see* ITHIEL DE SOLA POOLE, TECHNOLOGIES OF FREEDOM (1983).

pricing issues, with a heightened lobbying of all interested parties focused on policy makers.

## II. TECHNICAL CONCERNS: A CABLELABS CASE STUDY

From a technical perspective, the layered approach is a useful framework for designing and building network systems. Indeed, the technical specifications created at CableLabs are no exception; yet at the same time, they offer an illustrative example into the shortcomings of the layered model. The DOCSIS®, PacketCable™, OpenCable™ and CableHome® platforms can all be described with a layered protocol stack, though as shown below, it is not necessarily a simple description.

At the outset, the right question to consider is how the technical development process for these platforms might differ under a layered regulatory model. Today, it is the business requirements of the cable companies that are members of the CableLabs consortium that drive the development process. The cable companies, in conjunction with equipment manufacturers, design the platforms to best deliver cable services to consumers as defined by these business requirements. There is no particular concern given to the specific layers into which functionalities may fall, beyond the implications of such placement on the overall need for an efficient implementation to meet consumer demands.

As a result, CableLabs platform specifications span a number of layers, which in turn raises concerns about the application of a layered regulatory model. First, regulations might limit a particular service provider to functionalities allowed in a particular layer. Second, layered regulations require clear interfaces between all layers defined by the regulatory model. This spanning occurs today due to the *interdependency of the layers* – a particular functionality requires implementation in more than one layer – or the set of business requirements dictate the need for functionalities that occur in more than one layer. In this section, we review some of the layer interdependencies and cross-layer functionalities of the existing broadband platforms (DOCSIS, PacketCable and CableHome) on the cable network.[8]

The demonstrated interdependency of the layers raises major concerns, as the layered regulatory model could limit a particular service provider to functionalities allowed in a particular layer, or require clear interfaces between all layers defined by the regulatory model.

8. While not included in this discussion, similar layer interdependencies exist for functionalities necessary for the OpenCable platform that provides digital video services and separable security capabilities.

### *A. DOCSIS*

The DOCSIS specifications define the physical interfaces supported by cable modem and cable modem termination system equipment. These physical interfaces connect the individual end users with the provider service delivery environment. Figure 1 shows a simplified description of the protocol software stack of a cable modem, which in this case, provides a typical consumer with Internet access via an Ethernet port.[9] In a rough mapping to the four-layer model noted above, the physical (PHY) layer maps to the DOCSIS physical layer and Media Access Control (MAC) protocols, the network layer maps to the TCP/IP protocols, and the application layer maps to the network and security management applications. A cable modem contains no content software that maps to the content layer.

The heart of the DOCSIS specification prescribes the DOCSIS PHY and MAC protocols. But one should not overlook the higher-layer functionalities which inhere in the DOCSIS specification either.[10] Most importantly, DOCSIS includes network management and security profiles.[11]

The higher-layer capabilities in network management and security are essential to the fundamental operation of the cable broadband service.[12] As such, any regulatory model that would preclude the network

9. The software stack diagrams were provided by Ralph Brown, CableLabs.

10. *See* CABLELABS, DATA-OVER-CABLE SERVICE INTERFACE SPECIFICATIONS DOCSIS 2.0, http://www.cablemodem.com/downloads/specs/CM-SP-RFI2.0-I10-051209.pdf.

11. As regards network management, the Operations Support System (OSS) Interface Specification defines the network management services required within DOCSIS 2.0 by using the Simple Network Management Protocol (SNMP) to perform account, configuration, fault, and performance management functions. This specification defines the subscriber account management interface that allows cable equipment vendors to develop products that address the operational requirements of cable operators' subscriber account management in a uniform and consistent manner. This includes such essential capabilities as how to provision broadband service to customers, the enforcement of the subscribed service level agreements (SLAs), and implementation of usage-based billing. From the network layers perspective, SNMP is typically associated with the higher layers (*e.g.*, application, presentation, and session layers). Meanwhile as for security, the DOCSIS 2.0 specification includes a Baseline Privacy Plus (BPI+) interface that provides cable modem users with data privacy across the cable network, in addition to providing cable operators with a strong protection from theft of service. BPI+ protects against unauthorized access to the MAC layer by enforcing encryption of the MAC layer traffic flows across the cable network. The protocol employs a client-server model running the security application. In this way the security as defined in the DOCSIS 2.0 specification is another example of an application layer functionality required to support the link layer. *See* http://www.cablemodem.com/downloads/specs/CM-SP-BPI+_I12-050812.pdf.

12. Other higher-layer protocols in the DOCSIS specification include Trivial File Transfer Protocol (TFTP) for downloading operational software and configuration information, Dynamic Host Configuration Protocol (DHCP) to allocate IP addresses, and Time of Day (ToD) protocol to obtain the time of day.

operator from higher layer functions would *literally disable* the operations systems of the network operator. In addition, the network management and security functions are multi-layer, spanning the network and application layers without open interfaces at this layer boundary. These technical characteristics of the DOCSIS platform raise important and unanswered questions of how the delivery of cross-layer functionalities could be handled in a layered regulatory model.

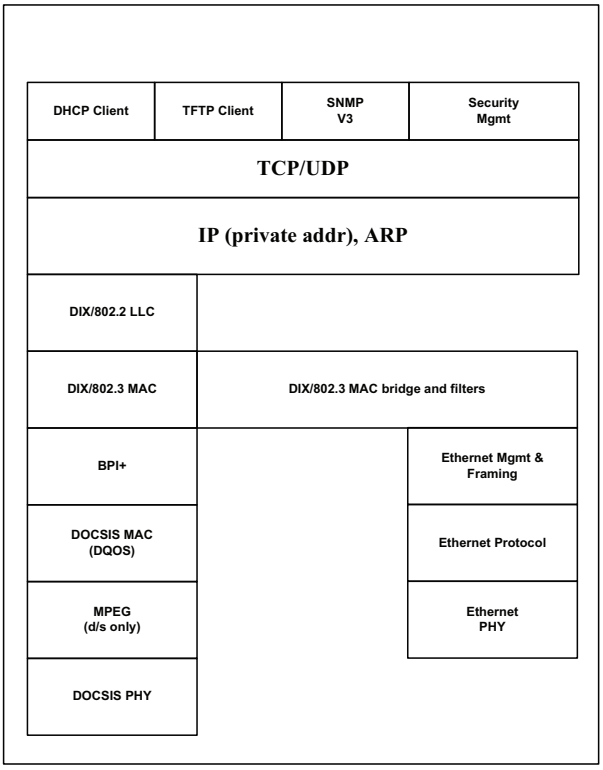


Figure 1: Software Stack of DOCSIS Cable Modem

### *B. PacketCable*

The PacketCable specifications define the interfaces required for a cable operator to provide Voice-over-IP (VoIP) and other multimedia services. PacketCable is a set of protocols developed to deliver communications services requiring quality of service (QoS) using packet-data transmission technology to a consumer's home over the cable network.

Figure 2 shows a simplified protocol software stack of a PacketCable Multimedia Terminal Adapter (MTA), which includes an embedded cable modem. The term embedded means that there is no

explicit interface included in the specification demarcating the boundary between the cable modem and the PacketCable software application in the MTA. In a rough mapping to the four-layer model, the PacketCable platform assumes the presence of DOCSIS for the physical and network layer protocols. PacketCable does specify a quality of service protocol at the network layer, along with the call signaling, voice codecs[13], client provisioning, billing event message collection, Public Switched Telephone Network (PSTN) interconnection, and security protocols that map to the application layer. An MTA contains no content software that maps to the content layer.

13. Coders/decoders—perform data conversions and are typically used in modems.

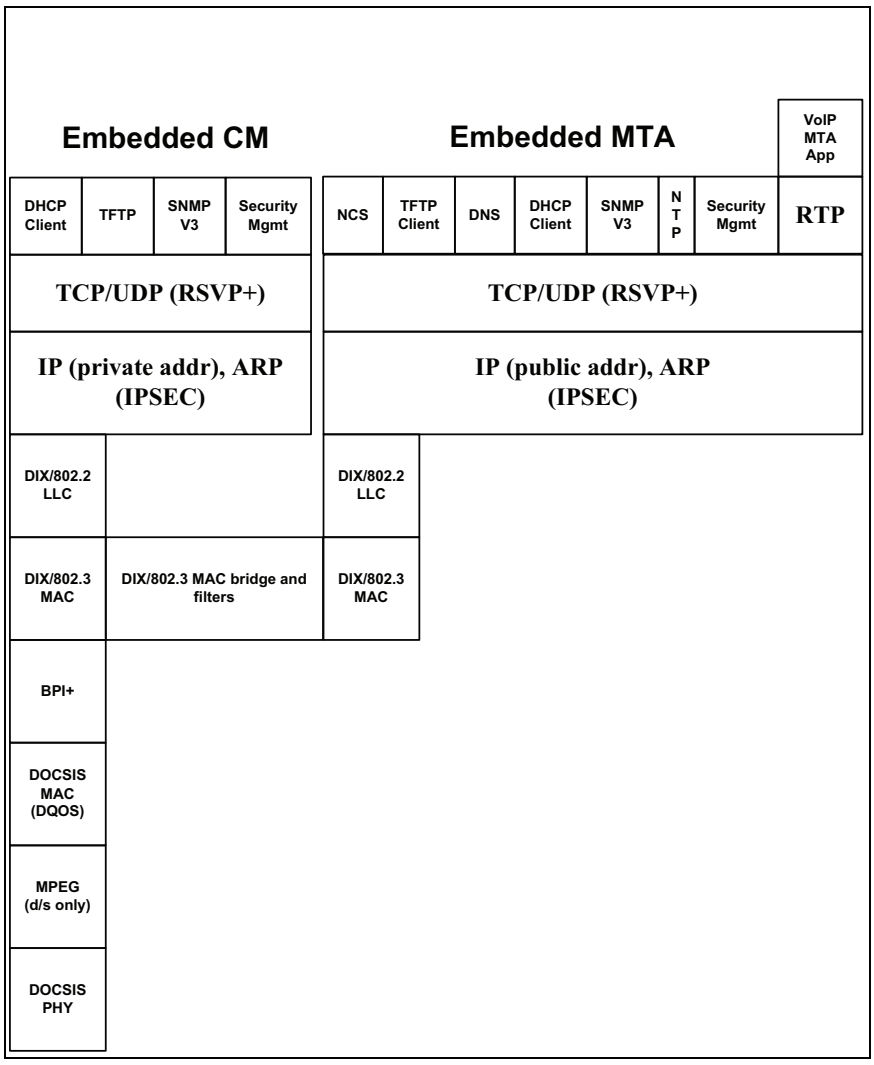


Figure 2: Software Stack of PacketCable MTA

The heart of the PacketCable specification specifies the VoIP application running in the Multimedia Terminal Adapter (MTA) in the subscribers' homes and the network elements required to support the application. For the purposes of this article concerning layered models, the PacketCable specification suite is illustrative of the problems in instituting a layered-based form of regulation. In other words, PacketCable is a poor candidate for layered regulation due to its cross-layer functionalities, its general purpose platform, and its underlying complexity.

First, an important cross-layer functionality in PacketCable is found

in the dynamic QoS specification, which specifies how an MTA can request a specific quality of service from the DOCSIS network.[14] The PacketCable QoS architecture is cross layer, as it specifies the necessary interaction between protocols in the network and application layers.[15] This cross-layer specification is required even though PacketCable, as a higher-layer specification suite, is built upon the lower-layer DOCSIS 1.1 specification. The important point is that even under the best of circumstances for a layered approach (*i.e.*, PacketCable specification riding over the lower DOCSIS specifications), cross-layer functionalities such as QoS are likely to occur. From a layered model perspective, the migration of functionality in one layer will often be tied to that of another.

Second, while the PacketCable VoIP specifications are customized for the delivery of residential telephony services, the PacketCable Multimedia architecture offers a general-purpose platform for cable operators to deliver a variety of IP-based multimedia services that require QoS treatment.[16] This architecture works only on the DOCSIS 1.1 portion of the network. All application managers and clients reside within a single cable-administered network. Despite the general layered approach of the specification, the expectation is that each multimedia application will probably require a profile, which may or may not have cross-layer implications depending upon the unique requirements of the application.

Third and finally, by specifying an MTA with an embedded DOCSIS modem, the PacketCable specification suite was made simpler by not having to specify the interface between the cable modem and the MTA. It was also completed in much less time since the complexities associated with a standalone MTA specification (*e.g.*, how to handle firewalls and network address translation) were not required to be part of the specification. Despite these efficiencies, a layered model would not allow the same specification approach, since the interface to customer premises equipment likely would have to be fully specified to permit several permutations of deployment beyond only embedded implementations. In other words, while a layered regulatory model may not preclude embedded implementations, it almost certainly would

14. *See* CABLELABS, PACKETCABLE™ 1.5 SPECIFICATIONS: DYNAMIC QUALITY-OF-SERVICE, http://www.packetcable.com/downloads/specs/PKT-SP-DQOS1.5-I02-050812.pdf.

15. As an aside, the PacketCable QoS architecture is based upon CableLabs' DOCSIS 1.1 specification, IETF's Resource reservation Protocol (RSVP), and Integrated Services Guaranteed QoS.

16. *See* CABLELABS, PACKETCABLE™ MULTIMEDIA ARCHITECTURE FRAMEWORK TECHNICAL REPORT, http://www.packetcable.com/downloads/specs/PKT-TR-MM-ARCH-V01-030627.pdf.

require a fuller set of platform specifications, which translates into a longer time to market for equipment and more complexity in the specifications.

In short, despite the fact that PacketCable is a "higher-layer" specification suite, this review of the PacketCable specifications raises some of the same cross-layer functionality concerns as noted for the DOCSIS platform. In addition, specifications that are fully compliant to a layered model can be more complex, and take longer to reach the market as they can require more interfaces to be specified than might otherwise be the case.

### *C. CableHome*

The CableHome specifications describe the IP-based architecture for managed home-networked services on the cable network through a DOCSIS cable modem.[17] Figure 3 shows a simplified protocol software stack of a CableHome Residential Gateway (RG), which includes an embedded cable modem. *Embedded* here means that there is no explicit interface included in the specification demarcating the boundary between the cable modem and the CableHome software application in the RG. In a rough mapping to the four-layer model noted above, the CableHome platform assumes the presence of DOCSIS for the physical and network layer protocols. CableHome does specify IP addressing requirements at the network layer, along with the home-networking management protocols that map to the application layer. An RG contains no content software that maps to the content layer.

A main focus of CableHome is to enable core DOCSIS and PacketCable functionality on home networks, with an additional focus on home network management capabilities. Like PacketCable, CableHome is also a multi-layer specification spanning the network and application layers (while DOCSIS spans these layers as well as the physical layer). This cross-layered functionality yields difficulty in imposing regulation based upon clear delineations between layers.

Yet CableHome represents a general layered approach in application. CableHome does not require a specific home-networking technology in the home. The expectation is that future network-layer profiles for specific home-networking technologies such as Wi-Fi or USB may be necessary to support certain services (like QoS) across the cable and home networks.

Finally, in specifying an RG with an embedded DOCSIS modem, the CableHome specification suite was made simpler by not having to

17. *See, e.g.*, CABLELABS, CABLEHOME 1.1 SPECIFICATION, http://cablelabs.com/projects/cablehome/downloads/specs/CH-SP-CH1.1-I10-051214.pdf.

specify the interface between the cable modem and the RG. It was also completed in much less time since the complexities associated with a standalone RG specification (*e.g.*, how to handle QoS) were not required to be part of the specification. While a layered regulatory model may not preclude this type of embedded implementation, it almost certainly would require a fuller set of platform specifications, which will have implications for a longer time to market and more complexity.

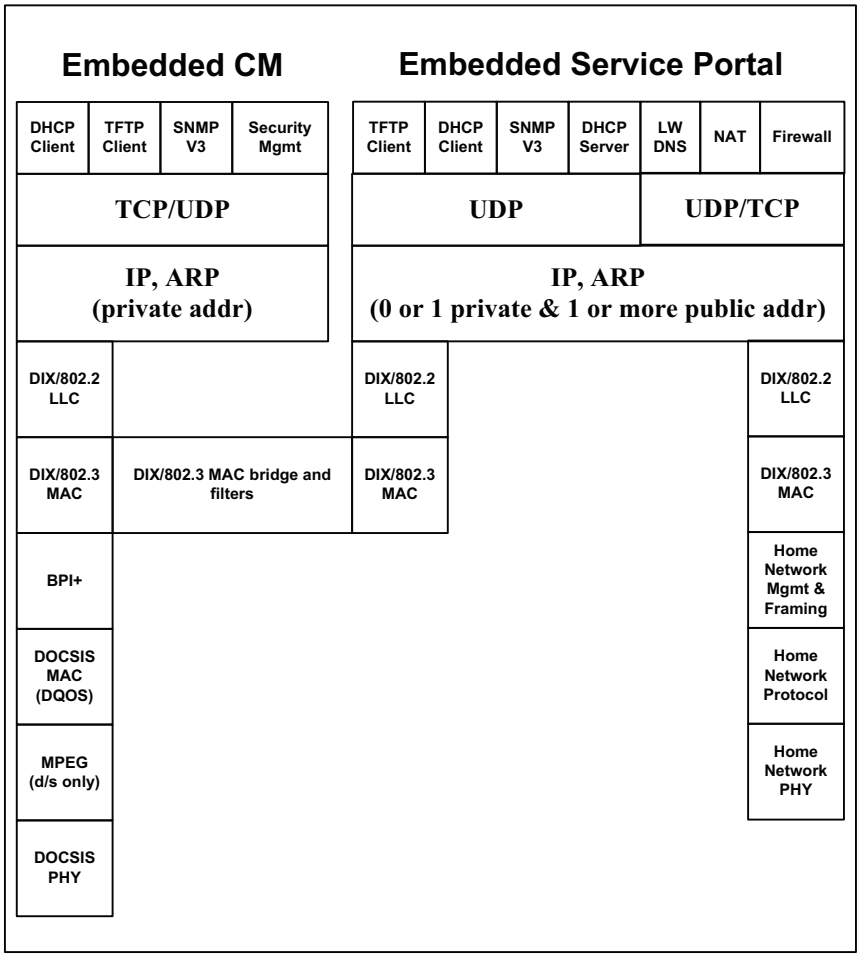


Figure 3: Software Stack of CableHome Residential Gateway

### *D. Technical Concerns Summary*

The above examination of the protocol stacks associated with the

technical platforms on cable should give the reader pause for four reasons.

First, software stacks are complex. The layered regulatory model sets a very high bar of technical competence for regulators. While the theory of layered networks provides a simple conceptual construct of how network systems work, actual implementations are much more complex to meet the business needs of the service providers.

Second, CableLabs platforms are not isolated in a single layer. The software stacks demonstrate how the DOCSIS, PacketCable, and CableHome platforms are all multi-layer by incorporating more than one layer into the specification suite. In other words, the functionalities required by cable operators to offer their services span multiple layers. Even though each layer is an important part of these cable platforms, a layered regulatory model that tries to organize services along exclusive horizontal layers will likely be problematic due to the significant amount of cross-layer functionalities.

Third, network design challenges will be presented by the erection of barriers across layers. One consequence of layer interdependence is that the technical evolution of the network is highly linked across layers. Changes in one layer need to be closely coordinated across all the other layers. A regulatory model that injects more players into the process of network evolution will make the task of planning network evolution very difficult. Moreover, a requirement for open interfaces at every layer boundary will make the specification more complex, and take longer to complete.

Finally, in a layered paradigm, regulators will be placed in the key role of designing the layered network systems through their frequent regulatory decisions. Consequently, regulators will have a primary role in controlling the rate of innovation on the layered networks. For example, bandwidth management on broadband networks has emerged as a key application for broadband network operators who must manage network usage to comply with consumer usage agreements. Bandwidth management tools have been developed with a wide range of capabilities, ranging from simple system that measure the traffic through a specific network point of control to sophisticated tools that will measure the traffic, decompose the traffic by flows, measure each flow, and restrict the passage of flows of specific types. Given the cross-layer, "traffic cop" nature of bandwidth management tools (*i.e.*, the interests of the layers are not aligned), it seems safe to predict this application, and others that are similar, would be highly controversial under a layered regulatory model and require a lot of attention from regulators. The delay caused by regulatory deliberations in this regard would serve to stifle innovation of cross-layer services.

Thus, because communications technology evolution will continue to span layers any regulatory intervention will have definite consequences. Most noticeably, by allowing regulators to select open access requirements at various points across the layers, technical neutrality is actually sacrificed in as much as technical winners and losers are no longer determined at the market. Further, by putting regulators at the vanguard of network evolution, delay and market frustration are bound to occur where advancement to market may only be accomplished through a regulatory approval.

## III. PUBLIC POLICY CONCERNS

The technical and economic issues presented by the layered model of regulation addressed above also equate to problems of public policy including the loss of neutrality in regulation, the imposition of a system of price regulation, and the subsumption of innovation to regulatory control.

As noted above, the layered model threatens to result in another attempt to impose price regulation under the guise of unbundling or open access requirements. The imposition of open access requirements on facilities-based carriers ultimately perverts the true price of various elements by regulatory machination with the overall result of inefficiency. In the past, similar regulatory unbundling efforts have met uneven success due to inherent complexity of pricing unbundled components in a public forum, the strident gaming of all participants in the regulatory process, and the lack of market-based checks and balances on the viability of unbundled elements. Layering advocates may argue that there is no better solution, but as will be discussed below, there is a better alternative in the form of promoting facilities-based competition and correcting for regulatory imbalances as they occur.

A central tenet of good public policy has long been to craft regulatory frameworks that are technologically neutral so that the market, not regulators, can ultimately decide upon the best technologies for deployment. However, the implementation of a layered model will place regulators in the position of selecting technical winners and losers instead of relying upon the market. In short, this sacrifices technical neutrality.

Regulations defining the layer interfaces must publish the specific technical elements to be maintained across layers, and any layered model ultimately selected by regulators constitutes a technical architecture in its own right. In turn, a loss of technical neutrality in regulation will arise as specific technical implementations are ratified. For example, regulators agreeing to implement a four-layer model versus a six- or seven-layer model will result in different technology being built and deployed by the different service providers for reasons of regulatory compliance. For this

reason, a layered regulatory model would be highly invasive, at least in terms of a managing communications markets, and would require expert application by regulators with a strong technical comprehension and strategic vision.

Finally, one of the most disturbing public policy concerns raised by the layered model is that regulators, as the ultimate decision-makers for what constitutes the layered model, will be in control of ongoing technical evolution of telecommunications networks. Even if regulators were to defer to technical standards bodies, any disputes arising from these organizations would ultimately have to be arbitrated by the regulators. Most proposed layered regulatory models presuppose the current layered structure of network systems based upon the Internet, and that such systems will remain relatively stable in the foreseeable future. This may or may not be true, but it would be the regulators' decisions directing the path of network evolution, not competitive markets featuring potentially disruptive technologies to the layers architecture.

With the regulatory intervention intrinsic to the layers regulatory model, public policy makers will need to establish a strong market failure to justify the high degree of market micromanagement associated with the implementation of the model with regard to how the networks will develop. With the steady increase in competition seen today in most telecommunications markets, imposition of a layers regulatory model would serve to provide regulatory intervention in the absence of market failure.

## CONCLUSION

In short, what is good for the engineer is not easily applicable to the regulator, at least not in terms of adoption of a rigid framework required for consistent regulatory decision-making. This is not a surprising observation as these two professions are trying to accomplish very different goals. Namely, engineers *build* networks to meet their clients' business and functional requirements; policy makers *regulate* communications services for the public benefit. Historically, when the two mix (*e.g.*, engineers try to build networks to achieve public policy objectives or policy makers design and dictate technical architectures),[18] inefficient outcomes are the common result. Thus, while it is true that engineers find a layered architecture useful in designing and building their network systems, the notion of applying this model for regulatory purposes is misguided and will likely result in an overly complex and rigid model upon implementation.

18. *See, e.g.,* Nat'l Cable Television Ass'n, 33 F.3d at 66.

As a result of these difficulties in successful implementation of a layered model, alternatives should be considered. Foremost among other paradigms of regulation is a regulatory model that promotes consistent facilities-based competition among service providers. In essence, this is the current policy in the United States. Competition among cable and telephone companies for broadband services is fierce, and the FCC has done a good job removing artificial entry barriers to allow more new service providers seeking to offer broadband services. Serious new broadband market entrants may emerge using broadband over power line, wireless broadband, or satellite technology. A public policy framework promoting facilities-based competition remains technologically neutral in that all technologies are given as reasonable prospects for success as is feasible by regulators. Regulators leave pricing to the competitive markets; they are not forced to intervene and make arbitrary judgments regarding how prices should be set.

The facilities-based model, however, requires some patience before the full benefits of competition can be realized. In the real world, it takes time to deploy the network infrastructure needed to support residential broadband networks, particularly on a nationwide basis. Indeed, it has taken time for digital broadband services to obtain its substantial market position, but it is now a viable competitor to traditional cable services.[19]

Thus, while the layered model may provide a useful framework for understanding the basic rudiments of telecommunications technology and network systems, it is not a useful regulatory model to tackle real-world public-policy issues. The few instances where proxies for layered regulation have occurred, such as UNEs in wireline telephony or the establishment of a video dialtone platform, have been failures despite the simplicity of this technology relative to advanced broadband networks.

Instead, it is important to turn to pause and look at the current market realities. Competition is steadily increasing in most telecommunications markets and, as such, imposing a layered regulatory model would be regulatory intervention in the absence of market failure. Such regulation would not only be unwarranted but likely to result in the unintended consequences including the loss of technological neutrality, unbundling obligations, and the stifling of future innovation.

19. Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming, *Eleventh Annual Report*, 20 FCC Rcd. 2,755, 2,766-68 (2005).

# MISUNDERSTANDING THE LAYERED MODEL(S)

DOUGLAS C. SICKER AND LISA BLUMENSAADT*



## INTRODUCTION

While the general idea of a layered policy model continues to gain attention (both positive and negative), it is clouded by the development of numerous competing models.[1] The original layered model, described

* Douglas C. Sicker is an assistant professor in computer science and telecommunications at the University of Colorado at Boulder. Lisa Blumensaadt is an attorney specializing in telecommunication policy and intellectual property. Professor Sicker would like to thank the following individuals for their assistance with this paper: Dale Hatfield, Phil Weiser, the University of Colorado Journal on Telecommunications and High Technology Law and in particular Eric Lentell, my article editor.

1. The proponents include: Rob Frieden, *Adjusting the Horizontal and Vertical in Telecommunications Regulation: A Comparison of the Traditional and a New Layered Approach*, 55 FED. COMM. L.J. 207 (2003); John T. Nakahata, *Regulating Information Platforms: The Challenge of Rewriting Communications Regulation from the Bottom Up*, 1 J. TELECOMM. & HIGH TECH. L. 95 (2002); Douglas C. Sicker & Joshua L. Mindel, *Refinements of a Layered Model for Telecommunications Policy*, 1 J. TELECOMM. & HIGH TECH. L. 69 (2002); Philip J. Weiser, *Law and Information Platforms*, 1 J. TELECOMM. &

fully later, and herein referred to as the "Sicker-Mindel-Cooper"[2] ("SMC") layered model, was intended as a tool for examining policy implications on technology and later evolved into a policy model intended to promote a technically neutral view of the various emerging network platforms.[3] It was originally intended to be an analytical framework; however, the original motivation and design of this model has been misinterpreted and restated by other authors.[4]

Meanwhile, the paper which did the most to promote the idea of a layered model, the Whitt-MCI paper,[5] also presented the most controversial interpretation of it. The Whitt-MCI Paper created a lot of attention for the layered model, and brought layered models under severe criticism, since it advocates for a specific regulatory outcome. In short, the Whitt-MCI paper advocates regulatory intervention at the physical layer[6] and the continuation of unbundling the incumbents' telecommunications networks[7]. While it offers an excellent overview of

---

HIGH TECH. L. 1 (2002); Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. TELECOMM. & HIGH TECH. L. 37, 39-40 (2002); Richard S. Whitt, *A Horizontal Leap Forward: Formulating a New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587 (2004); Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law* (University of San Diego School of Law, Public Law and Legal Theory Research Paper No. 55, 2003), *available at* http://ssrn.com/abstract=416263. The opponents and critics include: Raymond Gifford, *The Uses and Misuses of the Layered Model*, THE SKEPTICAL REGULATOR (August 2004), http://www.pff.org/irle/skepticalregulator/skepticalregulator2.3.html; David P. Reed, *Critiquing the Layered Regulatory Model*, 4 J. TELECOMM. & HIGH TECH. L. 281 (2006); J. Scott Marcus, *The Potential Relevance to the United States of the European Union's Newly Adopted Regulatory Framework for Telecommunications* (FCC Office of Plans and Policy, Working Paper No. 36, July 2002), *available at* ftp://www.fcc.gov/pub/Bureaus/OPP/working_papers/oppwp36.pdf.; Wayne T. Brough et al., *Free Ride: Deficiencies of the MCI 'Layers' Policy Model and the Need For Principles that Encourage Competition in the New IP World* (New Millennium Research Council Paper, July 2004), *available at* http://newmillenniumresearch.org/news/071304_report.pdf [hereinafter NMRC].

2. *See* Sicker & Mindel, *supra* note 1.

3. Douglas C. Sicker et al., *The Internet Connection Conundrum* (unpublished FCC Office of Plans and Policy, Working Paper, 1999) (on file with the Journal of Telecommunications & High Technology Law).

4. *See* Whitt, *supra* note 1.

5. *Id.*

6. *Id.* at 592 (stating "*the[MCI] Network Layers Model targets the lower network layers for discrete regulation* based on the existence of significant market power, rather than legacy service or industry labels. This framework concomitantly fosters maximum innovation by leaving otherwise competitive content and applications markets unfettered by regulation.") (emphasis added). The physical layer refers to the underlying physical infrastructure that carries communications signals, such as the cable and associated facilities carrying cable television signals.

7. *Id.* at 649. ("Section 251(c) of the Telecommunications Act of 1996, which requires the ILECs (Incumbent Local Exchange Carriers) to provide unbundled network elements ("UNEs"), can be an important legal mechanism in service of the [MCI] layers principle."). ILECs, a term created by the Telecommunications Act of 1996, are "local exchange carriers" that provided "local exchange service" prior to the enactment of the Telecommunications Act

prior work in the area, the paper concludes with a position that strongly aligns with the policy desires of competitive local exchange carriers (CLECs), specifically their desire to unbundle the local loop[8]. In turn, this position has met with great resistance by various segments of the policy community.[9] As a result, critics of the layered approach focus their energies on the shortcomings of the Whitt-MCI model, yet fail to engage in a rigorous discussion of the general concept of a layered policy model.

Subsequent to the SMC layered model other layered models were developed; however, these models differ in the division of the layers and how they view the value of the divisions. In particular, Whitt,[10] Marcus,[11] Werbach,[12] Reed,[13] Gifford[14] and the New Millennium Research Council ("NMRC")[15] examined layered policy approaches and developed variations or critiques of such models.

The goal of this paper is to demonstrate that a layered model is still a useful framework for policymaking in the current environment. Section II provides background on the original intent of the SMC layered model and describes the current regulatory model and the technical underpinnings of layered models (the Open System Interconnection [OSI] Stack and Transmission Control Protocol/Internet Protocol [TCP/IP] Suite). Section III reviews the details of the SMC layered policy model and summarizes and addresses the major points of critical analysis and provides a brief descriptive review of the other major layered policy models. It then discusses how the

---

of 1996, 47 U.S.C. § 251(h) (2005) [hereinafter 1996 Act]. They are commonly thought of as local telephone companies or the "Baby Bells," and are the long-existing owners of the physical local communications networks. This term is used in conjunction with the term Competitive Local Exchange Carrier (CLEC), which is a new local exchange carrier trying to compete with the well-established traditional local telephony service providers (ILECs). UNEs, or unbundled network elements, are discrete portions of a local exchange network that together make up a loop connecting the local telephone company office equipment to residential or businesses' communications equipment. UNEs were created by the 1996 Act and subsequently specifically defined by a Federal Communications Commission Order to engender competition in the provision of local communications services by allowing CLECs to make cost-based purchases of discrete portions of the physical local network that they needed in order to provide local communications services in competition with the ILECs without having to build out their own redundant physical network. 1996 Act, 47 U.S.C. § 251(c)(3) (2005); Implementation of the Local Competition Provisions in the Telecomm. Act of 1996, *First Report & Order*, 11 FCC Rcd. 15,499 (1996).

8. *See* Whitt, *supra* note 1, at 649.
9. NMRC, *supra* note 1. *See also* Reed, *supra* note 1; Gifford, *supra* note 1.
10. *See* Whitt, *supra* note 1.
11. *See* Marcus, *supra* note 1.
12. *See* Werbach, *supra* note 1.
13. *See* Reed, *supra* note 1.
14. *See* Gifford, *supra* note 1.
15. *See* NMRC, *supra* note 1.

SMC layered policy model, based on the layered structure of communications networks, is still valid and useful as a framework for examining policy implications. The section ends by articulating the ways in which the layered policy models remain relevant. The paper concludes in Section IV with a summary of the likely layers that will emerge in future regulatory frameworks.

## I. THE LAYERED MODEL

### *A. Original Intent of the SMC Layered Policy Model*

The SMC model began as a simple intellectual exercise with the intent to describe the way that networks actually operate for regulators wrestling with applying policy. Communications evolved into vastly different networks from those the existing regulatory framework was designed to address. Policymakers struggle to apply an outdated regulatory framework to the new communications networks, where the physical structure of the networks no longer fit the regulatory structure. Furthermore, segments of the network now operate under very different market conditions than existing regulations assumed. Joshua Mindel, Cameron Cooper and Douglas C. Sicker described the original layered model in an unpublished paper written in 1999 while working for the Federal Communications Commission (FCC).[16] Later, the concept evolved into an analytical policy tool, one in which networks were assessed in a technically neutral manner with a focus on detecting where market abuse might occur.

The original idea behind the layered concept was not about creating a new regime for regulation, but rather to function as an analytical tool for evaluating how to regulate evolving networks. The goal was to move toward technical neutrality and therefore, consistent treatment. This could be achieved through regulation based on the service, rather than of the network infrastructure that carries the service. An additional objective was to define a model where the application layer could continue to innovate by avoiding unintentional regulation.

### *B. Current Regulatory Structure – A Review*

The current communications regulatory structure is often described as a "silo" model, with regulation of a service closely associated with the underlying physical infrastructure on which a service is offered. There is a separate "silo" associated with each platform –wireline (twisted copper pair), cable (coaxial) or spectrum (wireless). For example, voice

16. *See* Sicker et al., *The Internet Connection Conundrum*, *supra* note 3.

(telephony) service delivered over wireline (copper twisted pair) is regulated under Title II – Common Carrier[17], but voice service delivered over spectrum (wireless) is regulated under Title III –Wireless. Thus the same service, voice, is regulated differently according to the physical infrastructure over which it is delivered. It is important to note that the regulation is not based on the platform or the service. For example Title II is a common carrier regulation, not necessarily a wireline or a voice regulation; however the platforms, the services and the titles have certainly become synonymous.

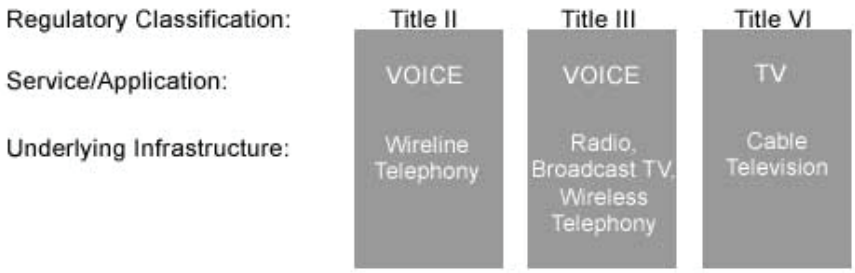


Figure 1. The current "silo" regulatory structure

This regulatory model was constructed around the technological and market conditions that existed at the time the laws were passed. For many decades, telephony service was a monopoly industry provided largely by one company, AT&T. It was thought to be far too expensive, unprofitable and inefficient for competing companies to redundantly lay tens of thousands of miles of wire and build the associated facilities to provide competing telephony service. Thus, modeling telephony regulation after existing "common carrier" regulation -like train service or a utility- made sense.

The system of regulation that developed around the evolving technology initially made a lot of sense. However, regulatory disparities began to emerge as cable television became a competitor to broadcast television and cellular (telephony) service began to replace wireline telephony use. Thus, similar services delivered over different infrastructure are regulated by disparate regulations.

The real difficulties, however, have developed with what many refer

17. *See generally* 47 U.S.C. § 202 (1989); 47 U.S.C. § 153 (1997) (stating "The term "common carrier" or "carrier" means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or in interstate or foreign radio transmission of energy, except where reference is made to Common carriers not subject to this Act; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier.").

to as "convergence" and the "digital revolution." Services are said to "converge" onto a single superstructure that could ride over all existing physical infrastructures –the Internet Protocol (IP) environment. In this environment, cable can deliver voice service and high-speed internet service, as well as television service; wireline telephony providers can deliver video service, high-speed internet service, and voice service; wireless telephony providers can also deliver internet service, streaming video and other services; and voice service, audio or video broadcasts, streaming video, audio downloads and more services can be delivered over the Internet, provided by ISPs -unaffiliated or affiliated with a cable company (over cable modem), or a phone company (over dial-up or DSL), or by a competitive provider (over leased dial-up or DSL facilities of the incumbent phone company). As each new service evolves, there is a need to classify it in order to determine under which regulations it falls. Regulating based on the infrastructure or associated title, however, no longer seems appropriate when each infrastructure can deliver a multitude of competing services. Entities provide competing services to consumers who do not generally distinguish between the same service delivered over different infrastructures. This differing infrastructure, however, causes these entities to operate under vastly disparate regulatory conditions.

The FCC tried to deal with regulation of nascent computer networks in *Computer Inquiry I*,[18] *II*[19] and *III*,[20] first by creating *basic* and *enhanced* service classifications. Basic services –"the common carrier offering of transmission capacity for the movement of information"[21] fell under common-carrier regulation and enhanced services remained unregulated.[22] This was the beginning of a layered model approach, as it established a separation of the transport network from services.[23] The Telecommunications Act of 1996 addressed this issue in legislation by defining a *telecommunications service* as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the

18. Regulatory & Policy Problems Presented by the Interdependence of Computer and Communication Servs. & Facilities, *Notice of Inquiry*, 7 F.C.C.2d 11, ¶ 1 (1966) [hereinafter *Computer I*].

19. Amendment of Section 64.702 of the Comm'n's Rules and Regulations (Second Computer Inquiry), *Final Decision*, 77 F.C.C.2d 384 (1980) [hereinafter *Computer II*]

20. Amendment of Section 64.702 of the Comm'n's Rules and Regulations. (Third Computer Inquiry), *Report & Order*, 104 F.C.C.2d 958 (1986) [hereinafter *Computer III*].

21. *Computer II*, *supra* note 19, at ¶ 93..

22. *Id.* at ¶¶. 100–01.

23. *See* Douglas C. Sicker, *Further Defining a Layered Model for Telecommunications Policy*, Paper Presented at the Telecommunications Policy Research Conference 2002, at 5, *available at* http://intel.si.umich.edu/tprc/papers/2002/95/LayeredTelecomPolicy.pdf.

facilities used"[24] and an *information service* as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[25]

Although these attempts were made to deal with a rapidly changing telecommunications landscape, minor regulatory overlays are not sufficient to fix the disparity caused by the inherited regulatory structure and the vastly changing communications environment. Thus, it is generally agreed that the current regulatory model no longer fits existing conditions. The layered model presents a possible framework with which to examine policy issues going forward.

### *C. Layered Model Description*[26]

In this section, we provide a brief overview of the basic ideas behind protocol layering. We also describe the Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models. We then describe the SMC concept of the layered model for policy.

#### 1. Protocol Layering

A computer network can be conceived of as the interconnections of computers that allow communication. The content, scope, size, speed and reliability of the network vary depending on its protocols and implementation. *Protocols* are pre-established rules or means of communication. They are simply a set of valid messages, rules and formats that govern the communication among peers.[27] Protocol layering is a common technique to simplify networking designs by dividing them into functional layers, and assigning protocols to perform each layer's task. Protocol layering produces a number of sub-functions, each with well-defined tasks. The concept of layering relies on breaking a complex task into smaller subsets, each of which addresses a specific issue. Each layer provides a well-defined set of services to the layers above it and depends on lower layers for its own operation, thus creating modularity.[28] The Internet protocols are arranged in essentially

24. 47 U.S.C. § 153 (46) (2005).

25. 47 U.S.C. § 153 (20) (2005).

26. This section substantially draws upon one of our original articles on the subject,, which more explicitly addressed the foundations of a layered model. *See* Sicker et al., *The Internet Connection Conundrum*, *supra* note 3.

27. For a detailed explanation of protocol Layering, *see* SRINIVASAN KESHAV, *Protocol Layering, in* AN ENGINEERING APPROACH TO COMPUTER NETWORKING: ATM NETWORKS, THE INTERNET, AND THE TELEPHONE NETWORK 67 (1997).

28. *See generally* Connected: An Internet Encyclopedia, *Protocol Layering*, http://www.freesoft.org/CIE/Course/Section1/4.htm (last visited Mar. 6, 2006).

independent layers with the Internet Protocol (IP) itself at the "waist" of the stack. The protocol stack broadens above the waist to support a wide range of transport and application layers including email, the Worldwide Web, file transfer protocols, remote login, etc. The protocol stack broadens below the waist to ride on a wide range of underlying networks using a variety of technologies including Ethernet, frame relay, ATM, ADSL, fiber optic systems, and so on. The modularity, coupled with well-understood specifications, facilitates the introduction of new technologies and new applications, thereby stimulating growth. Modularity also promotes an environment wherein providers compete with products that will interoperate.

2. Open System Interconnection (OSI) Stack

The International Organization for Standardization (ISO) created the seven-layer Reference Model of Open System Interconnection to describe networked systems. Each of these layers has a set of specific functions associated with it, as depicted in Figure 2 below:

**Physical:** covers the network hardware, physical cabling and signal specifications.

**Data Link:** attempts to make the physical link reliable and provides the means to activate, maintain and deactivate the link.

**Network:** provides for transfer of packets between end systems across a communications network.

**Transport:** provides a mechanism for the reliable, transparent exchange of data between end-points across a network.

**Session:** provides the mechanism for controlling the dialogue between applications in end systems, such as starting and terminating sessions.

**Presentation:** defines the format of the data to be exchanged between different applications and offers application programs a set of data transformation services.

**Application:** provides entry points for user programs to control transmission of data to and from other machines. It contains management functions and generally useful mechanisms to support distributed applications. [29]

29. For a detailed explanation of the OSI reference model and description of each layer, *see* WILLIAM STALLINGS, DATA AND COMPUTER COMMUNICATIONS 51-54 (6th ed. 2000).

### 3. Transmission Control Protocol/Internet Protocol (TCP/IP) Suite

The term TCP/IP (Transmission Control Protocol/Internet Protocol) suite actually refers to a whole family of protocols, of which TCP and IP are just two. TCP/IP, which began development in 1969 by the U.S Department of Defense Advanced Research Projects Agency (DARPA), is an industry-standard suite of protocols designed to provide internetworking. TCP/IP protocols map to a four-layer conceptual model also known as the DARPA model, named after the aforementioned U.S. government agency. The four layers of the TCP/IP suite are: Network Interface, Internet, Transport and Application. Each layer in the TCP/IP suite corresponds to layers in the OSI model.[30]

**Network Interface Layer:** The network interface layer is the lowest layer in the Internet reference model. It corresponds to the physical and data link layers of the OSI model. This layer contains the protocols used to deliver data to the other computers and devices that are attached to the network. TCP/IP was designed to be independent of the network access platform. In this way, TCP/IP can be used to connect differing network technologies such as Ethernet, ATM or Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies.

**Internet Layer:** This layer is responsible for routing messages through networks. The Internet layer is similar to the Network layer of the OSI stack explained earlier.

**Transport Layer:** The protocol layer just above the Internet layer is the transport layer. It is responsible for the reliability and integrity of the end-to-end communications. It is similar to the transport layer of the OSI stack mentioned earlier.

**Application Layer:** The application layer is the highest layer of the TCP/IP protocol stack. It maps to the upper three layers of the OSI model. It provides applications the ability to access the services of the other layers and defines the protocols that applications use to exchange data.[31]

The TCP/IP protocol suite is quite similar to the OSI reference model and each contributed to the other. The main differences between the OSI architecture and that of TCP/IP relate to the layers above the

30. *See* MICROSOFT CORP., INTRODUCTION TO TCP/IP, http://www.microsoft.com/ntserver/zipdocs/TCPIntrowp.doc (last visited Mar. 6, 2006).

31. *See* CISCO SYSTEMS, INC., UNDERSTANDING TCP/IP, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.pdf (last visited Mar. 6, 2006).

transport layer (layer 4) and those below the network layer (layer 3). OSI has both the session layer and the presentation layer, whereas TCP/IP combines them into the application layer. Also, TCP/IP combines OSI's physical layer and data link layer into a network interface level. In reality, the TCP/IP model is agnostic to what exists below layer 3; however, it is common to see it referred to as the network interface The figure below shows the basic layering approach in both the schemes.

The intention of the SMC layered model was to start with a model that technologists use to conceptualize the hardware and software associated with a network (i.e., protocol layers) and use this as a framework for describing a new way of viewing long term policy decisions. We originally examined the direct applicability of the TCP/IP prot ocol suite and the OSI reference model to this task. See Figure 2.

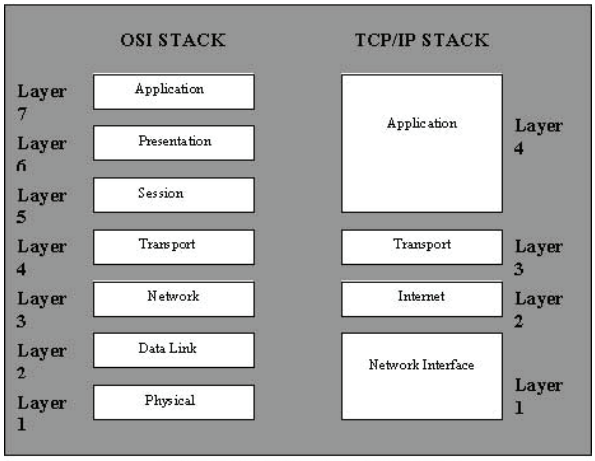


Figure 2. The OSI and TCP/IP Models

4. The SMC Layered Model as it relates to Policy

While other models are essential in developing the hardware and software associated with a network, they often fail to capture the reality of the policy issues or network and market conditions. In essence, there are layers in these models that do not directly relate to policy issues or market reality. However, by using a more simplified model, a more realistic model of network and market concerns is developed. Thus, the SMC layered policy model considers the layers that are typically associated with the various devices in the network and those related to policy issues or market realities. The layers in the SMC model represent

providers of services, not the protocols or the implementation of these protocols.[32]

Services and service providers are the focus of the SMC model, rather than those parties that might develop the products and services on behalf of the service providers.[33] The service layers distinguish among types of 1) physical services (e.g., access, transport), 2) application services (e.g., directories, caching, voice, electronic mail), and 3) content (e.g., music, video programming). These categories are described below:

***Physical service providers*** are providers of 1) Access and 2) Transport services, including both best-effort and QoS services.[34]

***Applications service providers*** are providers of application services that rely on underlying access and transport services and could be further subdivided into three subcategories: 1) directory service providers (e.g., DNS and other naming/numbering functions); 2) intermediate or middle service providers (e.g., multicasting and caching); and 3) end user service providers (e.g., voice, email, and hosting). One could argue that these three subcategories are distinct and should be treated as such, but this broad categorization is sufficient for this context. The point is to distinguish between the provision of a data delivery service and the applications that use or support the data delivery service.[35]

***Content providers*** are providers of content who rely on underlying Transport, Access, Application services. Examples of content include video, music, and telephony services.[36]

The SMC layered policy model distinguishes between a transport and access layer, where most models collapse this into a single transmission layer. Earlier work on the SMC layered policy model notes that "[t]he separation we describe between the access and transport providers maps to the design of networks."[37] The transport layer encompasses the "long-haul" or backbone portion of the network, which operates on large scale movement of data in a competitive market. Meanwhile the access layer encompasses the "last-mile," which is a fairly non-competitive market that uses different technology and operates on a much different scale. These are separate markets that operate

32. *See* Sicker, *Further Defining a Layered Model for Telecommunications Policy, supra* note 23, at 10.

33. One could also argue that software developers and consumers are also crucial to the deployment and use of the infrastructure, and should therefore be included in the framework.

34. *See* Sicker & Mindel, *supra* note 1, at 16.

35. *Id.*

36. *Id.*

37. *See* Sicker, *supra* note 23, *Further Defining a Layered Model for Telecommunications Policy*, at 12 (noting that "[e]ven future policy such as the Bill and Keep model maintains this division") (citing Patrick DeGraba, *Bill and Keep at the Central Office as the Efficient Interconnection Regime* (FCC Office of Plans and Policy, Working Paper No. 33, Dec. 2000), *available at* http://www.fcc.gov/osp/workingp.html).

fundamentally differently and exist under vastly different market conditions. As such, access and transport should be denoted by separate layers. However, in the future this distinction may become irrelevant. As stated in our earlier work,

The separation of the access network from the transport network . . . is critical to the success of this model. By making this division, the proper incentives could be introduced (through regulation or economic incentive) to encourage providers of the various services to interconnect on reasonable terms.[38] See Figure 3 below.

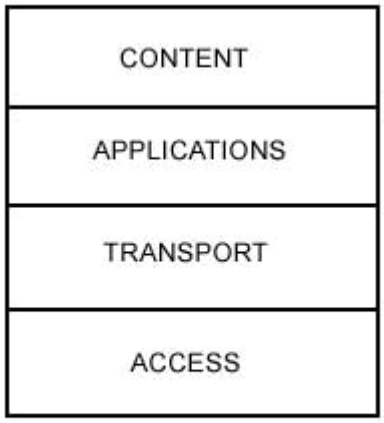


Figure 3.
The SMC Layered Policy Model

This layered stack provides a framework for systematic evaluation of the relationships between the layers. The important provider relationships are:

A - Access Provider to Access Provider
B - Access Provider to IP Transport Provider
C - IP Transport Provider to IP Transport Provider
D - IP Transport Provider to Application Service Provider
E - Application Service Provider to Application Service Provider
F - Application Service Provider to Content Provider
G – Internet Service Providers to Telecommunications Service Provider[39]

Relationships A through F are depicted in Figure 3a. An application service provider may directly connect with an access provider,

38. *See* Sicker, *supra* note 23, *Further Defining a Layered Model for Telecommunications Policy*, at 11.
39. *See* Sicker & Mindel, *supra* note 1, at 17.

but for purposes of simplification we leave this relationship out.

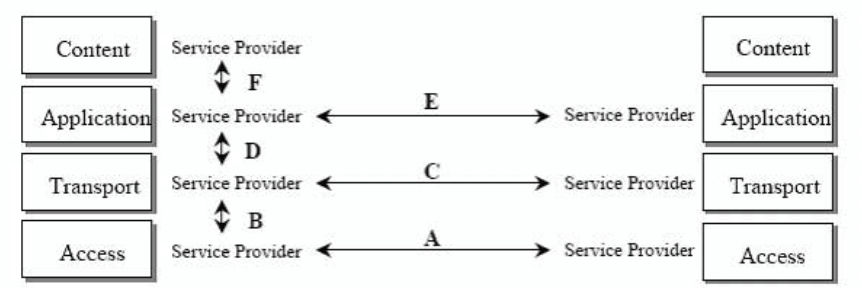


Figure 3a: Relationships among Infrastructure Service Providers

Figure 3a should be viewed as a conceptual model of the relationships between layers and service providers.

From a telecommunications policy perspective – and the perspective of this paper in particular – these are the relationships of primary interest. For example, an IP transport provider will use applications on their network, but since what they offer (to the public for a fee) is the transport service, the transport is the service of interest. Similarly, an application provider will employ network infrastructure (access and transport) to connect their applications to the public network, but the service is the application, not their network.[40]

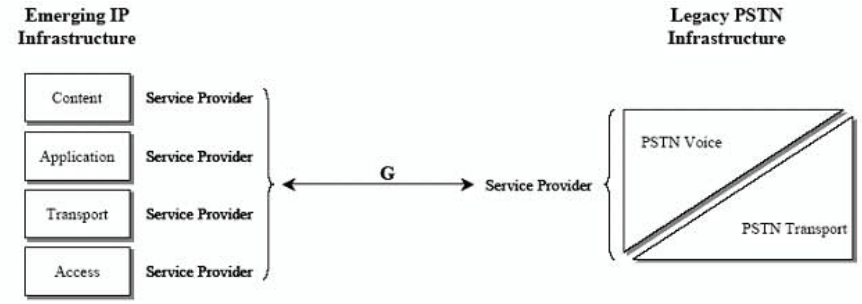


Figure 3b: Relationship between IP and PSTN Infrastructure Providers

Figure 3b depicts the relationship, G, between Internet Service Providers and Telecommunications Service Providers. The diagonal layering implies that PSTN voice and PSTN transport services are more tightly coupled than are the modular layers in the emerging IP infrastructure.

40. For more on the details of this model, *see* Sicker et al., *The Internet Connection Conundrum*, *supra* note 3.

In Figure 3b,[41] services that would be considered an application service in an IP context (e.g., SS7/IN and directory services) are in the upper diagonal, and those services that would be considered a transport service are in the lower diagonal. Both are considered telecommunications services in legacy PSTN regulation.

In summary, the SMC layered policy model concept was not about creating a new regime for regulation, but rather developing a tool for looking at networks in a more technically neutral and consistent manner. The model consisted of 4 layers, the access, the transport, the application and the content and stressed the notion of the application layer being a highly innovative layer; one that should be allowed to evolve with minimal regulatory interference, while preserving its open and developmentally accessible nature.

## II. REVIEW OF THE SMC LAYERED POLICY MODEL

This section summarizes and addresses the major points of critical analysis of layered models, as well as reviewing the critical differences of other layered policy models when compared to the SMC layered policy model. This section then goes on to discuss why a layered policy model is still a viable approach and why the SMC layered model remains the best approach for policymaking in the current environment.

### *A. SMC Layered Policy Model Description*

As discussed in detail earlier, the SMC layered policy model began by considering the OSI and TCP/IP models that technologists use to conceptualize the hardware and software associated with a network. The SMC model excludes layers that did not directly relate to policy or market concerns, with the layers in the SMC model representing services and service providers, rather than the protocols or protocol implementations.

41. *See* Sicker & Mindel, *supra* note 1, at 18.

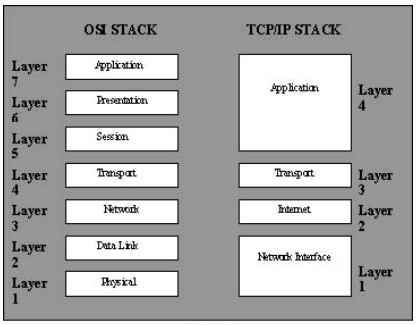


Figure 4

The ***Access and Transport layers*** represent providers of physical services. The ***Application layer*** represents providers of application services reliant on underlying Access and Transport services. Lastly, the ***Content layer*** represents providers reliant on underlying Access, Transport and Applications, including video, music and telephony services.

Critical to this model is the separation of the Access and Transport layers. As noted earlier, the Transport layer represents the "long-haul" or backbone portion of the network that supports large scale movement of data in a fairly competitive market environment. Whereas, the Access layer represents the "last-mile" portion of the network that operates on a much different scale, in a fairly non-competitive market environment, using different technology.

The separation of the Access and Transport layers is critical to a layered policy model since the representative networks operate fundamentally differently in separate markets and under vastly different market conditions. As such, separation of the Access and Transport layers allows for the proper incentives to be introduced, via regulation or economic incentive, to encourage these service providers to interconnect on reasonable terms. Importantly, the separate Application layer distinguishes between provision of a data delivery service (Access or Transport layers) and the applications that use or support the data delivery service. Also critical is that the SMC layered policy model stresses that the Application layer is a highly innovative layer that should be encumbered by minimal regulatory interference to preserve its innovation and open and developmentally accessible nature.

This is the essential framework of the SMC layered policy model. The goal of the model is to create consistency in policy. If used properly, a layered model will be helpful in minimizing or compartmentalizing regulation because it allows policy makers to consider regulation at each layer distinct from others, targeting only the appropriate layer. As such the SMC layered policy model itself does not advocate specific policy

positions. But, one may employ various tools within the framework, such as use of market power analysis and use of fines or additional obligations for anticompetitive exertion of market power or violation of interconnection rules.

### *B. Layered Model Criticisms and Differences*

Major points of critical analysis of layered policy models are reviewed here and addressed in relation to the SMC layered policy model. This section groups duplicate and overlapping criticisms together and reviews the assessment of them to more clearly delineate the critical issues with layered policy models and the answers to these criticisms.

*Criticism: Faulty assumption of* ***undue market power****, given the number of competing providers;*[42] *VoIP will only increase competition*[43]*; "Voice over Internet completely replaces traditional telephone calling;"*[44] ***Facilities-based competition*** *exists;*[45] ***UNE-P*** *is not creating facilities-based competition; Regulation of telecommunications industries is no longer needed;*[46] *Assumption of* ***monopoly power*** *of physical layer providers is incorrect when considering wireless and satellite technology advances and broadband over power line potential;*[47] *The layered model* ***criminalizes competition*** *by punishing those with undue market power;*[48] *Layering (a.k.a. unbundling) will degenerate into simple price regulation;*[49] ***UNE-P causes lack of investment*** *in DSL and the layered model would extend this investment uncertainty to all Internet companies in the Physical layer.*[50]

These criticisms are closely related and the same or overlapping support is used in addressing these points. First, mere numbers of competing providers is only one factor in determining market power or true competition. The statistics do not reveal that there is true competition and an assumption of ILEC market power is not unwarranted. CLECs only provide service over 18.5% of the total lines and only 25.8% of those account for their own local loop facilities (barely over 4% of the total lines), while 74% of their service is provided over

42. *See* NMRC, *supra* note 1, at 1-5.
43. *Id.* at 5.
44. *Id.* at 20.
45. *Id.* at 5.
46. *Id.* at 20.
47. *Id.* at 5.
48. *Id.* at 12.
49. *See* Reed, *supra* note 1, at 2.
50. *Id.*

leased ILEC UNEs or resale of ILEC services.[51]

Although mobile wireless subscriptions are just beginning to slightly outpace land lines,[52] this service is largely duplicative, with customers having both a land line and a mobile subscription and is not indicative of direct competition. Additionally, VoIP only offers service over 1.5% of the total lines.[53] Also, VoIP (as now generally offered) is not a complete replacement for traditional telephony service as the quality of service and reliability are not equivalent, and E911 features are only now being required and adopted. Similarly, the aforementioned rebuts the assertion that facilities-based competition exists in the current market and supports the contention that UNE-P is failing to create facilities-based competition. That said, it should be noted that only the Whitt-MCI model specifies use of UNE-P, as other layered policy models are more generalized frameworks that do not propose specific policy positions. In any case, as the above support illustrates, there is not meaningful facilities-based competition, suggesting that regulation of telecommunications or market opening measures may may still necessary. Further, regulations are often used to promote desirable goals, such as ubiquity of service, public safety, national security, education and other goals that may not be brought about naturally by market mechanisms.[54]

In addition, an assumption of monopoly power is not improper when considering the impact of advances in wireless, satellite technology, and broadband over power line on the telecommunications sector. Although there are advances in these emerging technologies, they have yet to translate into competition to voice service providers. Additionally, the support cited in the preceding paragraph on undue market power, shows an assumption of monopoly power in general (or at least great concentration of market power) in the access market is not an unfair assumption.

Layered policy models do not criminalize competition by punishing those with "undue market power." Although the Whitt-MCI model relies strongly on market power analysis, the SMC model merely views this as one tool that may be utilized within a layered framework and would only use this in the case of an anti-competitive exercise of market

---

51. FCC, Federal Communications Commission Release Data On High-Speed Internet Access Services, at 4-6 (December 2004), *available at* http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-tate_Link/IAD/hspd1204.pdf.

52. *Id.*

53. Rhonda Ascierto, *E911 Ruling May Raise VoIP Prices*, COMPUTER BUSINESS REVIEW ONLINE (May 23, 2005), *at* http://www.cbronline.com/article_news.asp?guid=1C0594D0-8FEF-4FC6-9A8B-061208534601.

54. *See* Sicker, *supra* note 23, *Further Defining a Layered Model for Telecommunications Policy*, at 2.

power, not mere possession of "undue" market power.[55] For the same reasons, the SMC layered policy model would not devolve into simple price regulation.

*Criticism: The layered model puts a ban on vertical integration / effects structural separation/ erects barriers between layers;*[56] *Regulators "could stifle innovation in cross-layer network technologies . . . [and] may preclude realizing economies of scale and scope across the unbundled interfaces;"*[57] *The layered model encumbers the transport layer, especially the last mile with regulation;*[58] *The Whitt-MCI model "places no value on economies of scope and vertical integration . . . leav[ing] the most costly portion of communications – building and operating the transport network under heavy regulation."*[59]

While the Whitt-MCI paper advocates maintaining rules that prevent ILECs from "closing interfaces between layers" or stifling higher layer competition,[60] even it does not imply that there should be a ban on vertical integration, nor does it (or any other layered policy model) effect structural separation. The SMC and other layered policy models also do not propose such a ban or imply structural separation, and they only consider control of multiple layers a factor in triggering additional obligations (such as pricing conditions) *if* market power is exerted in an exclusionary and anticompetitive manner. Furthermore, in contrast to erecting barriers between layers, using a layered policy model allows regulation to be readily compartmentalized and minimized by targeting only the appropriate layer.[61] For these reasons, a layered policy may not stifle innovation in cross-layer network technologies or preclude realizing economies of scale and scope across the unbundled interfaces.

Only the Whitt-MCI layered policy model extends UNE-type obligations to wire line broadband. Using other layered policy models may well result in removal, rather than extension of current regulation in

55. *See id.* at 20 (stating that, "while similar policy will be applied to all service providers, those determined as having significant market power will have additional obligations. When a player is determined to have significant market power, a pricing condition will be invoked. This condition will vary depending on power exerted; whether the player controls multiple layers or significantly controls a particular layer. For example, many cable and LECs would be viewed as significantly controlling the access layer. Other players, such as AOL/TW, would be viewed as operating in multiple layers.").

56. *See* NMRC, *supra* note 1, at 6, 12, 16, 23, 27-29.

57. Reed, *supra* note 1, at 2, 11.

58. *See* NMRC, *supra* note 1, at 5.

59. *Id.* at 21.

60. *See* Whitt, *supra* note 1, at 653.

61. *See* Sicker, *Further Defining a Layered Model for Telecommunications Policy*, *supra* note 23, at 9.

that similar services, regardless of the delivering infrastructure, would be viewed in a similar manner. Thus, cable, wireless and satellite broadband providers shall be considered competitors to DSL providers, possibly allowing policymakers to see sufficient competition within that layer. The same argument applies to the assertion that transport layer, especially the last mile, is encumbered by regulation by a layered policy model. This argument is true for the Whitt-MCI model, but not for other layered policy models.

While we agree that the Whitt-MCI model proposes unduly heavy regulation of the physical access layer and that physical network providers need a return on investment, it should not come at the expense of stifling competition in higher layers, *i.e.* facilities owners must not be allowed to shut out non-affiliated applications providers.[62]

*Criticism: "A layered policy model places too much control in regulators to "beneficently intervene" in the market and relies too heavily on antitrust law."*[63]

Although it is desirable to rely on market forces to provide optimal innovation and competitive consumer pricing and benefits, current market conditions (market consolidation, lack of reasonable interconnection agreements, and lack of facilities-based competition) do not allow for this. Furthermore, this criticism is applicable only to the Whitt-MCI model. Again, the SMC layered policy model mentions market power evaluation merely as a tool that may be employed within a layered framework.[64] Moreover the SMC model does not advocate threat of divestiture, as it is not likely to create the desired response, especially in any meaningful timeline. Rather, improved capability to monitor and fine those that violate pricing or interconnection rules is crucial.[65]

*Criticism: The model is a "gross simplification" of Internet elements with no appropriate reference to how those layers interact or relate;*[66] *A superior analytical tool for network engineers is not good for network regulators;*[67] *A layered model centered around the Internet does not*

62. *See* Sicker, *The Internet Connection Conundrum*, *supra* note 3, at 14.

63. *See* NMRC, *supra* note 1, at 8.

64. *See* Sicker, *Further Defining a Layered Model for Telecommunications Policy, supra* note 23, at 11, 20.

65. *Id.*

66. *See* NMRC, *supra* note 1, at 11.

67. NMRC, *supra* note 1, at 8. We note that McClure specifically reviews the Whitt-MCI layered model, and in the narrower context of use for Internet Public Policy only.

*capture all telecommunications.*[68]

First, the basis of the SMC layered policy model is not the Internet, but the TCP/IP model –these are not equivalent. Furthermore, the TCP/IP model is used only as a starting point. The layers in the SMC layered policy model are representative of providers of services, not protocols or protocol implementations of TCP/IP.

Inherent in the above explanation is that the SMC model is not the same model that network engineers use. More importantly, development of the SMC model extensively considered what layers relate to policy issues, real market conditions, and what layers are associated with relevant network devices and services.[69] Work on the SMC model identified no less than seven relationships between the layers and described and analyzed them in great detail.[70] In addition, numerous other considerations were made in developing the SMC model.[71] The criticism that a layered model centered around the Internet does not capture all telecommunications today is directly focused at the Werbach layered policy model, which advocates "reformulat[ing] communications policy with the Internet at the center . . . build[ing] our laws around the Internet, not the other way around."[72] In summary, the SMC layered policy model is not Internet focused, but used the TCP/IP model as a starting point for its development.

*Criticism: Loss of technical neutrality in regulation;*[73] *The need for technological neutrality should be explicitly added to the model.*[74]

Use of a layered policy model will bring technical neutrality to regulatory analysis by providing a framework where markets and competition are evaluated in a technologically neutral manner.[75] Thus providing consistency in that similar services in equivalent layers are viewed in a similar manner,[76] rather than viewing similar services

68. Marcus, *supra* note 1, at 1 (citing Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. ON TELECOMM. & HIGH TECH. L. at 38, 58 (2002)).

69. *See* Sicker, *supra* note 3, *The Internet Connection Conundrum* at 27-48.

70. *See* Sicker, *Further Defining a Layered Model for Telecommunications Policy*, *supra* note 23, at 17-18.

71. *See* Sicker & Mindel, *supra* note 1, at 81-83.

72. Werbach, *supra* note 1, at 38, 58.

73. *See* Reed, *supra* note 1, at 2.

74. J. Scott Marcus & Douglas C. Sicker, *Layers Revisited* (Sept. 25, 2005) (unpublished manuscript, presented at Telecommunications Policy Research Conference), *available at* http://web.si.umich.edu/tprc/papers/2005/492/Layers%20Revisited%20v0.4.pdf.

75. *See* Sicker & Mindel, *supra* note 1, at 5.

76. *See* Sicker, *supra* note 23, *Further Defining a Layered Model for Telecommunications Policy*, at 9.

differently because of their legacy classifications.

### *C. A Layered Policy Model Remains Relevant*

The SMC layered policy model is intended as a tool for examining communications policy issues and to move policy decisions to technical neutrality, and therefore more consistent treatment of providers of similar services. This is achieved by considering regulatory action based on providers offering similar services, rather than on which underlying infrastructure carries the service. An effect of employing the SMC layered policy model is that it minimizes regulation. In this way, the highly innovative application layer could retain its rate of innovation by avoiding unintentional regulation. In the same manner, unnecessary or unintentional regulation of the competitive market of the Transport layer is avoided by separating it from the non-competitive, high sunk-costs market of the Access layer. And any regulation of the Transport layer would not unintentionally include the Access layer since they are considered separately within the SMC model as they are separate markets that operate fundamentally differently and exist under vastly different market conditions.

## CONCLUSION: THE INEVITABLE LAYERS OF A REGULATORY FRAMEWORK

While the critics of the layered models are mostly accurate in their assessments, they are focused on only one of the models (the Whitt-MCI model) and fail to fully consider the other work in the area. Specifically, the SMC layered model withstands the criticisms leveled at the Whitt-MCI paper.

It remains to be seen just what direction the US will take in revising the 1996 Telecom Act, but it appears likely that steps will soon be taken to revise it. And while the debate continues concerning the value of a layered model, it is difficult not to believe that distinctions (and thus layers) will exist in what ever regulatory framework that is adopted. For example, it seems likely that the network that develops will separate the physical facilities from the applications and content that travel over them.

As we continue to move to a world where transport networks converge to offer broadband IP access, we will see these various networks supporting the same applications and content. As such, the network model will be one of access and transport networks at lower layers, with the applications and content that ride on these networks in higher layers. Even a policy model that ignores the difference between transport, applications and content will find itself faced with addressing these distinctions should a market abuse issue arise. Such analysis might

consider the abuse of dominance in one market (say access networks) or the tying of a transport network with an application or content. In this way, the final analysis will indeed be about layers, regardless of whether the policy model labels them.

# A DIGITAL AGE COMMUNICATIONS ACT PARADIGM FOR FEDERAL-STATE RELATIONS

KYLE D. DIXON & PHILIP J. WEISER*



* Kyle Dixon is Senior Fellow and Director of the Federal Institute for Regulatory Law & Economics at the Progress & Freedom Foundation ("PFF"). Philip J. Weiser is an Associate Professor of Law and Telecommunications, and the Executive Director of the Silicon Flatirons Telecommunications Program, University of Colorado. This Article stems from the report of the Federal-State Framework Working Group of the Digital Age Communications Act (DACA), which Kyle Dixon and Philip J. Weiser co-chaired. The authors thank all members of the working group—Robert (Bob) C. Atkinson, Kent Lassman, Douglas C. Sicker, Adam Thierer and Steven Titch—for their contributions and particularly acknowledge the very helpful efforts of Ray Gifford, President of PFF, both on this report and for his leadership on the DACA Project more generally (see http://www.pff.org/daca).

## INTRODUCTION

Drafting a statute that addresses the challenges posed by "digital age" communications requires thoroughgoing revision to the traditional role for not just federal, but also state regulation. The traditional "separate and dual" regulatory authority dating back to the Communications Act of 1934, and even the hybrid approach of the Telecommunications Act of 1996, must give way to a more consistent, principled appreciation for the purposes of administrative regulation and the technological realities of modern networks.

This article flows out of a Working Group report of the Digital Age Communications Act (DACA) project, in which various experts from around the country have examined and proposed solutions to pressing issues in communications reform. The overall DACA regulatory framework, which is rooted in competition policy,[1] calls for a reconception of the roles of both federal and state regulators.

First and foremost, the Working Group endeavored to follow DACA's paradigm shift from "legislative regulation" to "rule of law regulation." By this, the Working Group envisioned that telecommunications regulation – at whatever governmental level – would follow a more formal, largely adjudicatory method in accord with pre-announced legal standards and rules. The current legislative regulation model, by contrast, operates within the broad, undefined mandate of the "public interest" standard that lends itself to legislative-type rulemakings, informal procedures and murky compromises. A rule of law regulation model is better suited to a competitive environment, promotes investment (because of its regularity and predictability), and limits rent-seeking opportunities because its process is less open-ended and indeterminate.

Second, the Working Group reallocates the respective duties and powers between federal and state regulatory entities. In line with DACA's basic premises and current policy trends, the overall structure and direction of communications regulation outlined in this report is federal. This orientation reflects the need for a unitary regulatory framework that matches the technological reality of competitive, geographically unconstrained, packet-based networks. Likewise, the emphasis on a single federal framework reflects our judgment that communications policy should be a subset of general competition policy, which largely resides at the federal level. Finally, a single overarching federal framework is necessary to avoid patchwork regulation and

1. *See* PROGRESS & FREEDOM FOUND., PROPOSAL OF THE REGULATORY FRAMEWORK WORKING GROUP RELEASE 1.0 (2005), http://www.pff.org/issues-pubs/other/050617regframework.pdf.

spillover effects from state regulation.

In developing our report, the Working Group received a wide array of input, including contributions from a session of the National Association of Regulatory Utilities Commissioners. With that input, and with further deliberation among the Working Group members, we revised our earlier work[2] and have finalized our report. In so doing, we both refine some of our earlier conclusions and add some additional points specifically related to local government regulation of telecommunications services.

In this report, the Working Group proposes the following framework for state and local regulation in three broad areas:

*Rate Regulation*—States initially will retain the authority to keep a basic local residential service rate. All other state rate regulation and the attendant regulatory mechanisms, however, will be preempted in favor of a general competition policy mandate superintended by the Federal Communications Commission (FCC or Commission). The recommended statutory language contains a petitioning process whereby even this rate will fade away unless the FCC finds evidence of "unfair competition" pursuant to DACA's Title I—Regulatory Framework.

*Competition Policy Adjudication*—The Working Group is split on this issue. Some Working Group members prefer that all unfair competition adjudication take place under the auspices of the FCC and that states be precluded from acting as competition policy adjudicators. Other members hold that the FCC should have the discretion to delegate "unfair competition" adjudications based on allegations occurring *entirely within* a state to the relevant state commission.

*Consumer Fraud and Other Issues*—The Working Group is largely content with the current allocation of these duties, where the states may act consistently with a federal standard. The Working Group, however, prefers a more exacting standard than now exists under Section 332 of the Communications Act because it wants to prevent "spillover" effects from overzealous state regulation in the name of consumer protection. State authority to engage in "consumer protection" will thus be confined to "unfair or deceptive practices" under the Federal Trade Commission (FTC) Act model. In addition, the proposed legislation would delegate to states and localities authority to promote public safety and homeland

2. For the initial version of the Working Group's report, *see* PROGRESS & FREEDOM FOUND., PRELIMINARY REPORT OF THE WORKING GROUP ON FEDERAL-STATE FRAMEWORK RELEASE 1.0 (2005), http://www.pff.org/issues-pubs/books/050721daca-fed-state-report.pdf.

security and to manage public rights-of-way, subject to federal law and other constraints. New franchises are eliminated in favor of granting states discretion to impose streamlined, statewide certification requirements. Any state fees for access to rights-of-way would be limited to the costs of such access.

In essence, the Working Group concludes that federal law should set forth a coherent framework that circumscribes the role of state and local authorities so as to advance sound competition policy goals. In so doing, it recognizes that a basic local service rate retains both political and practical appeal during the initial stages of communications reform. Similarly, the Working Group believes that current state alternative dispute resolution procedures and other processes for solving consumer fraud problems work reasonably well. The group therefore retains these delegations as a matter of statute, but makes clear that state consumer protection efforts cannot spillover into adjacent jurisdictions or be used as a pretext for economic regulation.

In developing this framework, the Working Group endeavored to reach a reasonable consensus among its members as to how to develop a strategy for implementing the basic vision of the Digital Age Communications Act. Ultimately, however, no Working Group member or co-chair agreed with all aspects of this approach, although all agreed that it improved upon the Telecommunications Act of 1996's allocation of jurisdictional authority. Where possible, we highlight notable areas of agreement and the logic behind different trade-offs made by the Working Group. Notably, in the case of whether to delegate competition policy administration to state agencies, we could not reach a final resolution and set forth two alternative approaches.

## I. BACKGROUND

Telecommunications regulation raises both substantive and institutional questions. All too often, however, policymakers focus on the substantive questions—say, what standards to use to justify competition policy measures—at the expense of a more careful evaluation of the institutional mechanisms they might chose to advance those goals. In the case of the responsibilities assigned to federal, state, and local entities, the lack of careful thinking in developing the Telecommunications Act of 1996 led to legal uncertainty, tension between the different governmental authorities, and continuing litigation.

A thoughtful and practical framework for federal, state and local relations in this context must address two primary considerations.

*First*, the framework must decide the degree to which federal, state and local authority should derive from an integrated national scheme or,

alternatively, from distinct schemes that govern each separate jurisdiction. This degree of integration can be calibrated, among other ways, through (1) federal preemption of state or local regulation; (2) delegations of authority, possibly in nuanced ways that would require state and local regulatory authority to conform to federal legal rules; or (3) "savings clauses" protecting state or local autonomy from federal interference. Notably, a typical savings clause preserves authority "not inconsistent" with a law's regulatory goals. In this respect, the tradition of preserving state rate-making authority represents a notable departure from an integrated framework insofar as it prevents the FCC from setting policy related to "intrastate rates."

*Second*, the framework must address, in a self-conscious manner, the scope of state and local authority with respect to so-called "social policy goals" that are distinct from potential economic regulation. These goals may pertain to such things as consumer protection, public safety, homeland security and management of public rights-of-way. With respect to obligations imposed on providers to address social policy goals, an ideal framework would allow for some diversity and experimentation while precluding spillover effects or inconsistencies with federal law.

In the Telecommunications Act of 1996, Congress adopted what might be generously termed "a hybrid strategy." As to its mission of opening local markets to competition (accomplished through the regulation of interconnection and wholesale markets), Congress provided the FCC with residual authority to oversee all aspects of this regulatory program, inviting state agencies to interpret and implement federal regulatory policy. At the same time, Congress left intact the traditional protection of state regulatory authority codified by section 2(b) of the 1934 Communications Act. With respect to developing standards for economic and social policy matters, Congress largely elided over this distinction, leaving unsettled numerous matters related to the respective roles of state and federal agencies and paving the way for litigation and legal uncertainty.

The advent of digital technologies in general and the Internet, in particular, continue to undermine the legal distinctions embodied in the 1996 Act. On account of the Internet's transformative effect on communications markets and the clear trend of technological convergence, the historic distinctions between interstate and intrastate services are evaporating. Moreover, given that Internet services—such as Voice over Internet Protocol (VoIP)—are national (and even international) in scope, there are increasing risks associated with allowing states to regulate telecommunications outside a unifying federal regulatory regime. For social policy concerns, however, there is an increasing recognition that matters ranging from universal service

concerns to consumer fraud to E-911 and emergency services will require the involvement of state and local authorities, even if some national standards will be appropriate and necessary.

This Report, anticipating that the current Internet developments are only the beginning of a massive transformation in communications markets, proposes a new charter for federal, state, and local cooperation under a Digital Age Communications Act (DACA). This charter, as suggested above, would explicitly integrate federal and state authority, thus replacing the 1996 Act's less-than-self-conscious approach and its retention of section 2(b). Moreover, this charter would make clear, with important limitations, that state agencies should be given greater solicitude on matters of social policy than on economic policy. It is envisioned that this approach will facilitate thoughtful policy decisions that would be made by the actor in the best institutional position to do so.

## II. ALTERNATIVES TO AN INTEGRATED REGIME

Before explaining the virtues and powerful rationale for an integrated regulatory system, we will first outline its two polar alternatives: (A) the historic system of separate and dual authority; and (B) a federal preemption model. For the reasons explained below, we found each alternative lacking in fundamental respects. Though we present these alternatives as polar opposites, we do not mean to present a false dichotomy or a means to make our integrated model more respectable. (Indeed, some members preferred the preemption option with respect to competition policy issues.) Rather, the poles of preemption, on the one hand, and separate and dual authority, on the other, serve to illustrate the conceivable models for a federal-state framework going-forward.

### *A. Unconstrained State and Local Regulation*

Since the enactment of the Communications Act of 1934, federal telecommunications law has emphasized that state agencies must be permitted to regulate "intrastate" telecommunications services. Indeed, Congress enacted section 2(b) of the 1934 Act[3] to reverse the Supreme Court's decision in the so-called *Shreveport Rate Case*,[4] which provided broad authority to the Interstate Commerce Commission to regulate

3. This section reads "nothing in this chapter shall be construed to apply or to give the [FCC] jurisdiction with respect to . . . charges, classifications, practices, services, facilities, or regulations for or in connection with intrastate communication service . . . ." 47 U.S.C. § 152(b) (1934).

4. Houston E. & W. Tex. Ry. Co. v. United States [hereinafter *Shreveport Rate Case*], 234 U.S. 342 (1914).

telecommunications.[5] In particular, the *Shreveport Rate Case* concluded that the Interstate Commerce Commission could regulate intrastate telephone service because of its effect on interstate commerce.[6]

To limit the scope of federal authority, the 1934 Act instituted what has become known as a "separations" model, under which states are free to regulate the so-called "intrastate" aspects of communications unless it would be "impossible" to separate those aspects from interstate services. From 1934 to 1996, regulatory agencies and the courts frequently considered where to draw the line between federal and state authority,[7] with the United States Supreme Court ultimately setting forth the logic and requirements of the separations model in 1986 in *Louisiana PSC v. FCC*.[8] In so doing, the Court recognized that the 1934 Act's regime was unstable, noting "while the Act would seem to divide the world of domestic telephone service neatly into two hemispheres . . . in practice, the realities of technology and economics belie such a clean parceling of responsibility."[9]

In the 1996 Act, Congress did not address clearly the jurisdictional relationship between federal and state authority, leading to a round of litigation as to whether the classic model of separated authority applied to the initiative of promoting local competition through the regulation of interconnection and wholesale markets. In *Iowa AT&T v. Utilities Board*, the Supreme Court made clear that the 1996 Act's new requirements followed what is generally referred to as "cooperative federalism."[10] Nonetheless, the 1996 Act left section 2(b) in place, allowing state agencies to maintain complete control over "intrastate" services. This regime, as the Supreme Court's *Louisiana PSC* decision anticipated, has faced constant pressure from a dynamic marketplace whose services increasingly do not follow geographic boundaries. Thus, for this model to function going forward, federal and state regulatory authorities would need to develop a re-energized use of a "separations process" that, among other things, would allocate jointly used resources

5. Louisiana Pub. Serv. Comm'n v. FCC, 476 U.S. 355, 372 (1986) ("[Section 2(b)] was proposed and supported by the state commissions in reaction to what they perceived to be the evil of excessive federal regulation of intrastate service such as was sanctioned by the *Shreveport Rate Case*.").

6. *Shreveport Rate Case*, 234 U.S. at 353.

7. *See, e.g.,* N.C. Util. Comm'n v. FCC, 537 F.2d 787, 793-95 (4th Cir. 1976) (upholding FCC preemption of state regulations that would impede implementation of federal CPE interconnection requirements).

8. 476 U.S. 355 (1986).

9. *Id.* at 360.

10. 525 U.S. 366 (1999). For a description of cooperative federalism in the context of the 1996 Act, *see* Philip J. Weiser, *Cooperative Federalism, Federal Common Law, and the Enforcement of the Telecom Act,* 76 N.Y.U. L. REV. 1692 (2001), *available at* http://lawweb.colorado.edu/profiles/pubpdfs/weiser/CoopFederalism.pdf.

between the two jurisdictions in a manner fit for a technologically dynamic era.[11]

*Advantages.* Creating a zone in which states can regulate unconstrained by federal law has certain advantages. Along the lines that motivated the enactment of section 2(b) in 1934, a separations model respects the longstanding tradition of a separate sphere for non-federal regulation and thus adheres to the ideal of a "dual federalism." Moreover, this approach seeks to minimize the degree of coordination (and thus litigation or other conflict) between state and federal regulators because such coordination would be limited primarily to managing the separations process. In so doing, this approach emphasizes the value of state experimentation in developing local solutions and remaining accountable for their success (or failure). This approach both minimizes the risk of a single suboptimal national policy and facilitates the development of optimal regulatory solutions that can be adopted nationwide.

*Disadvantages.* The separations model also involves significant disadvantages. Although this model respects the value of state autonomy, it downplays the importance of interstate spillovers that are often better addressed through national regulation. In particular, for industries like communications that substantially involve activities that cross city and state lines, it is often difficult to preserve an independent regulatory sphere for states and localities to regulate outside of a federal regulatory framework.

The evolution of modern communications technology continues to undermine the case for state autonomy and bolsters that of the value of national oversight as an aspect of interstate commerce. As former California PUC Commissioner Susan Kennedy put it, "[t]he interstate nature of many emerging communications technologies argues strongly for a national regulatory framework."[12] In particular, multiple technological trends are eroding the once clear distinction between local and long distance services: the cost of communicating is becoming more distance insensitive; geographic boundaries are irrelevant to emerging technology; intelligence and functions are migrating away from the central office (the delocalization of the central office); the relevant

11. The FCC has largely declined to address the challenges in reforming the separations process for a new technological era. *See* Jurisdictional Separations Reform and Referral to the Federal-State Joint Board*, Notice of Proposed Rulemaking*, 12 FCC Rcd 22,120, 22,126 (1997) (noting that "today's network architecture and service offerings differ in many important ways from the network and services" that spawned current separations process, constructed at a time when services were provided "through a regulated monopoly").

12. Susan Kennedy, Federal and State Regulatory Responsibilities in a National Communications Market 1 (2005) (unpublished manuscript, available at http://www.naruc.org/associations/1773/files/LTF_susankennedypaper.pdf).

networks as well as the services that ride on these networks are increasingly comprised of numerous component parts (e.g., those offered by different providers); packet-routed networks are becoming more prevalent than circuit-switched networks; and the application (e.g., voice) is becoming more independent and separate from the network.[13]

In sum, the ability to regulate intrastate services distinctly from interstate ones is increasingly difficult to sustain with respect to digital age communications networks, which increasingly revolve around the Internet and wireless technologies. As the FCC stated in concluding that Vonage's Voice over Internet Protocol offering was subject to federal jurisdiction, communications services are increasingly "designed to overcome geography, not track it."[14] Thus, any attempt to allow states and localities to try to "isolate" and then regulate aspects of these services risks distorting or impeding the evolution of modern communications networks as well as creating significant spillover effects. Finally, the competition policy maxim of promoting competition, not individual competitors is not always grasped by state regulators (or federal ones for that matter).

### *B. Preempted State and Local Regulation*

For industries that are national in character and involve interdependent services, Congress often adopts a national regulatory regime that leaves no role for state administration. Such regimes, ranging from the regulation of retirement benefits (in ERISA) to airlines (in the Airline Deregulation Act of 1978), place a high value on uniformity and predictability, thereby discounting the possibility that local administration could produce better results either through closer proximity to consumers or the possibility of experimentation with distinct approaches. In telecommunications, there are only limited elements of a preemption strategy, such as the 1996 Act's categorical stance against state-created barriers to entry.[15]

*Advantages.* The advantages of the preemption model mirror the disadvantages of the unconstrained model and vice-versa. The preemption model gives full weight to national policy to set forth a uniform policy and process to govern all communications networks and services, regardless of boundaries. By providing such uniformity, this

13. Douglas C. Sicker, *The End of Federalism In Telecommunications Regulation?*, 3 NW. J. OF TECH. & INTELL. PROP. 130 (2005), *available at* http://www.law.northwestern.edu/journals/njtip/v3/n2/3.

14. Vonage Holding Companies Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission, *Memorandum Opinion & Order*, 19 FCC Rcd. 22,404, ¶ 25 (2004).

15. *See* 42 U.S.C. § 253 (1996).

model would seek to maximize regulatory certainty and promote investment and innovation in new, cross-boundary networks and services. Moreover, the preemption model arguably eliminates the need for coordination among federal, state and local regulators, thus avoiding the complexities of separations.

A preemption model can overcome certain parochial interests that tend to take root with state regulation. Though there is not an entirely clear answer as to where consumer-harming rent-seeking is more pervasive, a casual survey of state regulatory activity – from airlines, to intrastate trucking, to motor vehicle dealers, to various professional licensing schemes – suggests that state regulation can be more easily and cheaply turned to benefit private, rather than public, ends. This is not to say that federal regulation is devoid of rent seeking. The history of the FCC itself belies such a claim. Nonetheless, the opportunities for forum shopping and costly state-by-state regulatory lobbying campaigns appear to be lessened, or at least refocused, in a preemption model.

There is also historical precedent recommending state preemption. Preemption of state regulation under a uniform deregulatory federal scheme resulted in large consumer welfare gains in other network industries: airlines, trucking, railroads and natural gas production. In those cases, preemption allowed the interests of consumers to triumph over the interests of regulated industries, which often act as the fiercest defenders of state regulation because the regulation can be turned to their advantage.

*Disadvantages.* Preempting state and local regulation downplays the values of regulatory federalism. By wresting power from states, this approach would disrupt state resources already devoted to telecommunications regulation, thereby generating dislocation and a significant re-orientation in telecommunications policy. This shift of authority would downplay the value of the states' institutional competencies and underestimate the challenges that would arise from the lack of federal resources and competencies to address all circumstances in which government involvement might be warranted. In particular, state agencies are already using administrative law judges and adjudicative-like procedures (along the lines envisioned by the Regulatory Framework set forth in Title I) more effectively than the FCC. Finally, a preemption approach precludes states and localities from experimenting with different regulatory solutions, even where state and local involvement may aid (or at least not hinder) the achievement of federal policy goals.

If the nature and conditions in telecommunications markets were relatively uniform, say, along the lines of airline safety standards, a preemption approach would not raise many of the above concerns. But, in reality, the economics of telecommunications networks underscores

that their rollout and use—along with the associated competitive consequences—differs between jurisdictions. In particular, given the notable variations in population density and economic wherewithal across the U.S., the relevant marketplace fundamentals are likely to differ considerably. Indeed, despite the impact of wireless and broadband technologies, the cost characteristics of local networks will remain distance and terrain sensitive for the foreseeable future. Consequently, this view holds that sound regulation will require sensitivity to local conditions that can best be achieved through a continued reliance on state and local authorities. Notably, a belief that states can effectively recognize and implement competition policy standards consistent with local conditions rests on an assumption of the competence and fidelity of state commissions toward a "rule of law" regulatory model. This relies on an empirical judgment about state regulatory commissions' respective abilities and histories, which given a wide variance in performance, is not indisputably clear.

Despite the appeal of a federal regulatory framework, the rationale for a continued state role cannot be ignored. The conditions that allowed for broadly preemptive federal roles in other network industries are not present in communications. For one, in no industry, save communications, has the state role in rate regulation—and specifically rate regulation in pursuit of "universal service" goals—been so pervasive. This means that state reliance interests remain strong for some continued regulatory role. The ultimate question is whether states have the capacity and ability to act to enhance consumer welfare under a competition policy framework. This requires a predictive judgment about the ability of state regulation to transform from a legislative regulator to a rule of law regulator.

The ability of states to transition to a regime guided by rule of law values colors one's enthusiasm for a more preemptive or integrated regime. Significantly, however, the preemptive model is not free from criticism on this ground, as there is reason to believe that the FCC cannot be easily transformed from a legislative to a rule of law regulator. In particular, the legislative regulation model the FCC now follows has a large constituency supporting it and it will not die without a fight. Accordingly, the predictive judgment as to which regulatory institutions can make the transition to a rule of law model more effectively is not immediately clear, meaning that involving states in competition policy judgments provides the important benefit of enabling diverse institutions to make the transition to a rule of law model at the same time and to create benchmarks for one another to follow (or avoid).

## III. AN INTEGRATED REGIME OF FEDERAL AND STATE AUTHORITY

The most significant debate among Working Group members focused on a choice between establishing an integrated regime of federal, state and local authority or, alternatively, broad preemption of state and local regulation. Such broad preemption no doubt would eliminate many of the shortcomings arising from the current statute's attempt to divide federal, state and local authority into separate spheres. Broad preemption also, however, would ignore the strong interests, institutional competencies and other practical considerations weighing in favor of some ongoing state and local involvement.

Upon reflection, the Working Group concludes that a self-conscious commitment to an integrated regulatory framework would best promote sound telecommunications policymaking. Under such a model, states and localities would be permitted to regulate only within spheres authorized by the federal government. This authority involves both an explicit delegation of authority—as exists, for example, under the 1996 Act's interconnection agreement regime[16]—and a tolerance (through a "savings clause") for states to act in ways that do not affect other states and are "not inconsistent" with federal regulatory policy.[17] In essence, this model reflects a "cooperative federalism" strategy that involves federal, state and local regulators in implementing broad federal policy goals.[18] As outlined in the introduction, we envision three distinct approaches for addressing (A) the extent to which state agencies should continue to set local "intrastate" rates; (B) whether and how states should help manage competition policy other than rate regulation (e.g., interconnection); and (C) how much discretion state agencies should enjoy in protecting consumers as well as addressing social policy goals. We will address each in turn.

### *A. Rate Regulation*

The historic role played by section 2(b) of the Communications Act of 1934 was to protect state authority from federal oversight. During an era when the separation of responsibility between federal and state

16. *See* 42 U.S.C. §§ 251, 252 (1996).

17. *See* 42 U.S.C. § 261(c) (1996). This proviso states: "Nothing in this part precludes a State from imposing requirements on a telecommunications carrier for intrastate services that are necessary to further competition in the provision of telephone exchange service or exchange access, as long as the State's requirements are not inconsistent with this part or the Commission's regulations to implement this part."

18. For a thorough discussion of cooperative federalism regulatory regimes, see Weiser, *Cooperative Federalism, Federal Common Law, and the Enforcement of the Telecom Act, supra* note 10, *passim*; Philip J. Weiser, *Towards A Constitutional Architecture for Cooperative Federalism*, 79 N.C. L. REV. 663 (2001); Philip J. Weiser, *Chevron, Cooperative Federalism, and Telecommunications Reform*, 52 VAND. L. REV. 1 (1999).

authority could be managed reasonably well, this approach enabled state agencies to maintain their authority over an island of "intrastate rates." This model, however, is not built for an era of Internet Protocal (IP)-enabled services where different broadband facilities support bundled offerings of services that—even for the once "local telephone service"—routinely cross state boundaries and are intricately related with one another. Consider, for example, that with the rapid declines in transport costs, many competitive providers are already relying on switching equipment far from the local calling area in question. In a world where the geographic endpoints of a call can be easily determined (as was the case in the traditional circuit switched environment), the classification of intra-state versus inter-state services could be accomplished without much difficulty (regardless of how the call was routed). But with the advent of IP services (such as Voice over Internet Protocol) and an increasing reliance on wireless networks, the location of one or both ends of a telephone call is increasingly difficult to determine.

In calling for the abolition of the section 2(b) approach, we are mindful that state oversight of ratemaking questions has played an important role in telecommunications policy. In particular, state authorities have undertaken local fact-finding and have addressed concerns about the reasonableness of the rates charged for telecommunications services on a market-by-market basis and whether they are constrained by local competition. Moreover, we recognize that many state legislatures and state agencies are thoughtfully re-examining the merits of continued rate regulation for markets increasingly characterized by competitive entry.

The Working Group is also mindful of the damage that overextended state rate regulation can cause. In most states, the rate structure did not derive from any measure of the cost of a given service, but rather as part of a universal service scheme. Thus, state rates were, and often remain, geographically averaged without regard to cost, as well as pervaded by cross-subsidies benefiting rural and residential consumers and burdening urban and business consumers. In turn, this rate structure offered distorted price signals to new market entrants in the wake of the Telecommunications Act of 1996. Accordingly, the state-regulated rate structure induced upstream distortions in the regulated wholesale rate structure until there was little hope of discovering a "market" price anywhere in the communications sector. A truly competitive, market-driven communications market will thus eschew rate regulation at both the retail and wholesale level, unless absolutely necessary.

The Working Group embraces a two-prong approach to rate regulation. First, for the most part, all future rate regulation is lifted and

heretofore impermissible.[19] Second, as an initial matter, rate regulation of basic local services that fall within the definition of a service supported by universal service under Section 254(c) of the 1996 Act—i.e., are viewed as essential utility type services—are grandfathered until the conclusion of state and federal proceedings to determine whether such rate regulation is justified in specific markets.[20]

The Working Group sees the initial retention of a basic service rate as a concession to immediate practical and political considerations, and therefore we also enact a petitioning process whereby this rate may also be ended in favor of a market process. Specifically, for the grandfathered basic services eligible for continued rate regulation, the Working Group proposes a mechanism for parties to petition for either the lifting of current regulation or the imposition of new regulation. In particular, any petition to reform current rate structures must be filed with the relevant state agency. That agency will have 270 days to act on this petition, and to determine whether its regulatory regime is consistent with DACA's Title I unfair competition standard, before it is deemed granted. Whether the petition is denied, granted by a decision, or granted by operation of law, any party can appeal such an outcome to the Federal Communications Commission. In the event that a party appeals a state agency's decision, the FCC will have 180 days to determine whether or not the presence or absence of state regulation is appropriate based on Title I's "unfair competition" standard. If the FCC fails to act within that time, any aggrieved party can file a petition directly with the U.S. Court of Appeals for D.C. Circuit.

In calling for an evaluation of rate regulation of basic telecommunications services based on whether it is justified under an "unfair competition" standard, we envision the development of a competition-based justification for rate regulation through a "common law-like" process involving the state agencies and the FCC. At a minimum, this process would call for real world market analyses and sensitivity to the continuing development of new forms of competition to traditional wireline telephony. That said, to the extent "unfair competition" exists in certain markets, this process would offer state agencies an opportunity to continue to perform their traditional role of protecting consumers from unreasonable rates for essential

19. The obvious exception is, as discussed below, any rate regulation justified under DACA's Title I's "unfair competition" standard.

20. The grandfathered state rate regulation for basic services and services supported under Section 254(c) is not meant to provide an ongoing lever for continued rate regulation, even if the definition of supported services under 254(c) (or its statutory successor) expands. Rather, this provision is meant to be a strict grandfathering clause. Only basic service rates in effect at the time of the passage of this DACA can remain in effect. Of course, a state on its own initiative can cease regulating this rate as well.

telecommunications services.

In recommending the approach set out above, we recognize the appeal of the alternative model of requiring all rate regulation to be lifted immediately (or within the very near term), with rate regulation being reimposed only where, when, and to the extent an aggrieved party can demonstrate consumer harm that can be remedied only by rate regulation.[21] Although this approach has much to commend it, we conclude that—particularly given the close scrutiny now being applied to most state regulatory regimes—it would cause more transitional difficulties than create consumer benefits through the lifting of unnecessary regulation. To be sure, we recognize the artificiality of many regulated rate structures, but we believe that a politically prudent, fact sensitive, and more gradual adjustment process will be a superior means of correcting unjustified rates and transitioning to a more rational regulatory strategy.

Yet another model of rate deregulation would retain the basic service rate, as the Working Group does, but sunset that rate by a date certain, thus doing away with the petitioning process.[22] The Working Group considers this a second-best alternative to the current petitioning process because it accomplishes the necessary goal of eliminating distortionary state rate regulation. However, the Working Group also believes that under a unified framework that encompasses all communications providers – large and small, urban and rural – there may be some ongoing need for continued regulation of a basic service package for certain customers still served only by a single provider. Thus, we would anticipate that most basic rate regulation would fall to the wayside under the petitioning process, but could still hold out that it might exist in small rural pockets of the country for an indeterminate time in the future.

A final model that the Working Group considered, but opted not to adopt, would preempt all rate regulation, including the basic service rate, and leave any subsidy questions (which the basic service rate represents) to a targeted universal service system. This solution has some attraction because it eliminates the ongoing distortions in the communications markets that a below-cost basic service rate represents. It further serves the goal of equity between providers because for the most part persistence of this basic service rate represents an ongoing subsidy

---

21. *See* Robert C. Atkinson, Dir. of Policy Res., Columbia Inst. for Tele-Information, Report at Remedies for Telecom Recovery II: What Can the Government Do to Help Recovery? (Oct. 29, 2004), http://www.citi.columbia.edu/research/recovery2/CITI_RegulatoryUpdate04.pdf.

22. *See, e.g.,* Raymond L. Gifford & Adam Peters, *A Model State Act for Communications,* 11.21 PROGRESS & FREEDOM FOUND. PROGRESS ON POINT § 4(a)(3), at 14 (2004), http://www.pff.org/issues-pubs/pops/pop11.21modelstate.pdf.

obligation for the incumbent to its basic service customers. There is, therefore, a strong policy rationale for doing away with all rate regulation and addressing particular universal service needs for those in need through a targeted universal service program. In the end, the Working Group opted to retain the basic service rate as the necessary political tradeoff for broader rate freedom. To be sure, the pure market-driven policy perspective would eliminate all state rate regulation and only subject freely set rates to the broader competition policy inquiry. But we anticipate that the basic service rate grandfathered here will be of little importance to the broader communications market as it evolves, and that in any event it will be petitioned away in most competitive areas of the nation's market within a reasonably short period of time.

In no event does the Working Group intend this grandfathered rate to evolve forward to include new packages of services that might someday be defined as "basic." Stated simply, no new services are to be brought within the ambit of state rate regulation unless the FCC concludes that such an approach is warranted under the regulatory framework. Significantly, with respect to any *future* evidence of "unfair competition," DACA's Title I—Regulatory Framework provides considerable discretion regarding how to remedy that behavior. As to the exercise of this discretion, the Working Group presumes that a remedy of rate regulation for any service, including basic local service, would only be imposed if it was the most effective one available.

In sum, we emphasize that the general preemptive approach toward rate regulation eclipses traditional state regulatory activities except where absolutely necessary. Thus, save for a basic service tariff and local exchange maps to define that basic service area, all other traditional state regulatory activities are exchanged for the competition policy standard. Under this approach, the classic issues associated with tariff-based regulation (and the concomitant protection of the filed-rate doctrine), such as rate cases, cost allocation proceedings, cost studies and general ongoing regulatory supervision, will fall by the wayside.

### *B. Competition Policy*

Under the Telecommunications Act of 1996, state agencies have played a crucial role in implementing the law's regulatory mandates. Unfortunately, the FCC and the state agencies have often failed to adopt a thoughtful and self-conscious approach to regulatory federalism. Rather, regulatory federalism often has served merely as another argument for parties to make opportunistically. The challenge for a new statutory framework—or even in managing the current one—is to develop a set of clear principles that do not lend themselves to continued

*ad hoc* and inconsistent application.[23]

Under the FTC-like model proposed by the Regulatory Framework Working Group, there is the critical question of how to implement what are almost certainly going to be fact-specific judgments that may well, in at least some cases, benefit from local fact-gathering and experimentation. There are two possible models that can be conceived for dealing with particular competition policy implementation questions.

First, there is a model where all questions are subsumed within the federal agency. This is how the Federal Trade Commission handles "unfair competition" inquiries, through the FTC's main office in Washington, D.C. and through its regional offices. Likewise, the Federal Energy Regulatory Commission considers interstate jurisdictional electric issues using its own administrative processes and administrative officers. This model clearly makes competition policy a federal prerogative and avoids the jurisdictional wrangling that the 1996 Act has provoked. Furthermore, it follows the historical models of airline, interstate trucking and natural gas deregulation, where states were precluded from an ongoing role in regulating these industries. In so doing, it solves the problem of states sometimes acting in a capricious or parochial matter, a problem that has been identified specifically in a "new economy" competition policy context by Judge Richard Posner.[24] Finally, there are exclusive fields of federal law already, such as bankruptcy, copyright and patent law. Accordingly, making communications policy exclusively federal is not unprecedented, even with a decent respect for

---

23. Philip J. Weiser, *Cooperative Federalism and Its Challenges*, 2003 MICH. ST. DCL L. REV. 727, 728-29; *see also* Atkinson, *supra* note 21, at 10.

24. *See* Richard A. Posner, *Antitrust in the New Economy* 10 (Univ. of Chicago, Working Paper No. 106, 2000), *available at* www.law.uchicago.edu/Lawecon/WkngPprs_101-25/106.Posner.pdf. (As Posner explained:

> I would like to see the states stripped of their authority to bring antitrust suits, federal or state, except under circumstances in which a private firm would be able to sue, as where the state is suing firms that are fixing the prices of goods or services that they sell to the state. (In other words, only their power to bring *parens patriae* suits would be abrogated.) States do not have the resources to do more than free ride on federal antitrust litigation, complicating its resolution; in addition they are too subject to influence by interest groups that may represent a potential antitrust defendant's competitors. This is a particular concern when the defendant is located in one state and one of its competitors in another, and the competitor, who is pressing his state's attorney general to bring suit, is a major political force in that state. A situation in which the benefits of government action are concentrated in one state and the costs in other states is a recipe for irresponsible state action. This is a genuine downside of federalism. The federal government, having a larger and more diverse constituency, is, as James Madison recognized in arguing for the benefits of a large republic, less subject to takeover by a faction. I am not myself inclined to make a fetish of federalism.)

*Id.*

federalism.[25]

An alternative model uses state resources to help implement a unitary federal regulatory scheme. Notably, in the environmental regulatory arena, there is a regular use of state regulatory resources to supplement federal oversight. Such use of state resources is at the federal agency's sole discretion and must be within the state agency's state-authorized powers, but it is a known model within administrative regulation. Health care regulation and funding also quite often adhere to this model through a "waiver federalism" approach. Under a "waiver federalism" strategy, the federal agency sets the general guidelines and rules, but a state is free to petition the federal agency for a waiver from the general rules and implement its own program.[26]

The extent, if any, of federal delegation of competition policy authority to states proved to be the most controversial of the Working Group's issues. A contingent of the Working Group argued for keeping states out of competition policy issues altogether, fearing inconsistent outcomes, rogue decision making, and disparate processes. An equally strong Working Group contingent argued for a narrow delegation to states to hear matters specifically and solely affecting their given state. This delegation authority resurrects the old pre-DACA "intrastate" category as the defining parameter of potential state delegated jurisdiction. At the same time, a delegation strategy recognizes that states have adjudicatory systems already in place (and ones more developed than the FCC's) and that a degree of decisional heterogeneity is not an "intolerable inconsistency," but rather can sometimes provide illumination on close competition policy questions (as well as procedural strategies). Finally, proponents of some delegation authority argued that the states' adjudicatory capacity might be needed to avoid backlogs and logjams at an overburdened FCC conducting true administrative adjudication for the first time.[27]

In the end, the Working Group could not reach a conclusive determination on this issue, but instead decided to define the parameters of the choices and delineate the specific contours of a limited delegation

25. This divided Working Group should hasten to point out, however, that these exclusive federal legal enclaves of bankruptcy, copyright, and patent are matters assigned to the federal government by the U.S. Constitution.

26. Waiver federalism models are most often used in situations like Medicaid funding where the federal and state governments are using matching dollars to fund a given program. Communications regulation in the pure regulatory sense is obviously different, but there are parallels in universal service policy.

27. As the report of the Regulatory Framework working group pointed out, a separate working group is focusing on institutional reform, including proposals to modify the structure of the FCC. So, the use of the term "FCC" here and elsewhere in this report is meant only to refer to the sector-specific regulator, however it is ultimately constituted. It is not meant to imply that the agency necessarily should remain in its current form.

model.

1. The No Delegation Model

The "no delegation" model is quite simple: all competition policy questions for all jurisdictional communications providers remain exclusively within the purview of the FCC and its administrative adjudicatory arm. Thus, all claims of unfair competition would be tried and worked out before the FCC. This would include broad, interstate questions about a general "net neutrality" mandate, as well as specific questions about whether a small 100 line rural phone company was abusing a terminating access monopoly. By envisioning that the FCC would determine all such issues, this model would require some form of local FCC branch offices or provision for local determinations of such matters.

The no delegation model ensures a unitary federal regulatory scheme for electronic communications services, and avoids heterogeneous decision makers with varying policy agendas.[28] Therefore, the no delegation model should, in theory, provide more national certainty as to the competition policy rules governing electronic communications networks and also streamline regulatory costs and proceedings into a single agency (i.e., the FCC).

Similarly, the no delegation model should at the very least narrow the available forums for rent-seeking and other untoward manipulation of the regulatory process. Moving from a "legislative regulation" model to a "rule of law" regulatory model suggests an aggregate move from more to fewer decision makers and toward more adjudication and less rulemaking. These factors counsel a single, unitary regulator implementing its decisions consistently across the nation. A no delegation model accomplishes this goal.[29]

28. This is only true of course as a formal matter. Within a single agency, there can of course be divisions and disparate agendas, most notably among professional staff and political appointees. Nonetheless, the theory of a unitary agency accountable to the president's appointees should be more likely to generate consistent outcomes than multiple state agencies, with different political allegiances and disparate competencies.

29. In fairness, it should be noted that the no delegation model also makes the FCC's faithful implementation of competition policy law and rules all the more important. Competition policy, understood as maximizing consumer welfare, still has sufficient breadth and doctrinal disputation to allow latitude to the regulator to be more or less intrusive in electronic communications services markets. It is sometimes argued that a single national rule that is bad is preferable to 50 different rules of disparate quality. This sentiment may be more a function of dissatisfaction with the current dual jurisdiction regulatory system than a considered view of what a uniform "bad" national rule might mean. One can imagine any number of catastrophic regulatory actions by an FCC disinclined toward implementing competition policy.

2. The Limited Delegation Model

The limited delegation model would be similar in concept to, but ultimately much narrower and circumscribed than, the 1996 Act's regulatory framework. Under this model, the DACA would provide an opportunity for the FCC to delegate authority to state agencies to implement its competition policy, consistent with a particular issue within a particular state. This delegation would entail several distinct elements. First, for a state agency to accept a delegation of federal authority, it would need to conclude (and the FCC would need to agree) that it enjoys legal and practical competence to administer the particular inquiry envisioned by the FCC.[30] This determination could include an evaluation of the ability of a state to follow a particular procedural approach. Such determinations would not be subject to a collateral attack or an interlocutory appeal. The use of this threshold requirement serves several purposes—(1) it ensures that state agencies are not "commandeered" into a federal regulatory program; (2) it underscores that state agencies must enjoy appropriate legal authority to implement federal law; and (3) it acknowledges that at least some state agencies may need to develop new practical abilities (say, economic and technical expertise) before taking on more challenging competition policy tasks.[31] To the extent that a state agency is either not able or willing to perform the delegated tasks, the FCC shall assume the appropriate responsibility. Because the issue delegated to a given state would have to involve just that state, the FCC could not use this delegation authority to "punt" tough issues it did not want to have to decide to the states.

To appreciate the mechanics of this approach, consider the case of an alleged terminating access monopoly being abused by a small, rural carrier within a given state. In that case, the state agency would need to conclude that it enjoyed the legal and practical ability to apply whatever competition policy-based standards the FCC developed to determine

30. This approach to delegation underscores what the Working Group considers a robust sensitivity to federalism concerns. In particular, states – and specifically state law – would have to embrace state administration (it need not necessarily be a utility or public service commission) of a federal regulatory regime. By calling for a self-conscious decision by states to accept a federal delegation, states will be able to evaluate the opportunity cost, weighting the direct cost versus the desire for control, of participating in this federal regime. For a discussion of these issues, *see* Weiser articles cited *supra* note 18.

31. For a discussion of the first two issues, *see id.* For concerns related to the latter, *see* Raymond L. Gifford, *Regulatory Impressionism: What Regulators Can and Cannot Do,* 2 REV. NETWORK ECON. 466, 477 (2003) (arguing that many state agencies "do not have the time, resources, or abilities to innovate or found new schools of competition policy"), *available at* http://www.rnejournal.com/articles/gifford-RNE_10_final.pdf. The "legal competence" prong is not a *pro forma* certification either. A robust federalism respects state law sufficiently to require states to have authorized their utility commission or other regulator under state law to participate in implementation of a federal statutory framework.

under what, if any, conditions a particular access pricing practice would be anticompetitive. By allowing a state to make and enforce its judgments, the FCC could foster creative experimentation in areas where the optimal approach was less than clear.

The second aspect of the limited delegation jurisdictional regime is the recognition that any explicit FCC delegation of authority to state agencies will often also entail some form of an implicit delegation of authority. This implicit delegation will often take the form of a "latent ambiguity"—i.e., a policy question that, although not apparent on the face of the matter, becomes clear in its application. To address such issues, state agencies would be authorized—but not required—to certify issues to the FCC for resolution. This "certification procedure" could also be used by state agencies to request flexibility not initially granted by the FCC (i.e., a waiver from the federal regulatory requirements).[32] The FCC would be required to decide such matters within 120 days and such decisions would be subject to appeal to the U.S. Court of Appeals for the D.C. Circuit. As to a state's resolution of any matter delegated to it by the FCC (either explicitly or implicitly), any party to the decision could appeal the state agency's decision to the FCC. If the FCC failed to act on such petition within a timely manner, any aggrieved party could file a petition for review with the D.C. Circuit.

To provide a mechanism for state agencies to alert the FCC of their interest in developing competition policy measures (such as the terminating access monopoly case discussed above), they would be required to first file a petition outlining the initiative in question and their reasoned basis for doing so. If the FCC failed to act on this petition within 90 days—either to endorse the measure or to bar it—the proposed proceeding would be deemed permissible. Notably, an FCC decision to allow a state to proceed to implement a competition policy measure would only imply that the FCC has made a preliminary judgment that any measure adopted by the state as a result of such proceeding is "not inconsistent" with DACA's regulatory framework. Such an FCC decision would neither immunize the subsequent state agency decision from challenge in federal district court nor prevent the FCC from later concluding that the measure in question is inappropriate. Rather, such a failure to act can be best analogized to a decision by the Supreme Court to deny a petition for certiorari, which expresses no view on the merits and leaves open the possibility that it will consider the question in a later case. Indeed, like the option to expressly tolerate

32. Such a waiver procedure is a frequently used aspect of the Medicaid cooperative federalism regulatory program. *See* Judith M. Rosenberg & David T. Zaring, *Managing Medicaid Waivers: Section 1115 and State Health Care Reform*, 32 HARV. J. ON LEGIS. 545 (1995).

different approaches, a decision by the FCC not to embrace or reject a particular regulatory measure can serve to foster experimentation in areas that are either complex or not well understood by regulatory authorities.

We emphasize that the delegation of adjudicatory authority to state agencies and the subsequent "appellate" process through the FCC and D.C. Circuit Court of Appeals is intended to follow administrative adjudicatory procedures and to reinforce DACA's commitment to a rule-of-law oriented regime.[33] In so doing, this regime distributes adjudicatory resources to handle both a large number of cases as well as complex inquiries that will turn on specific factual determinations. Moreover, this regime ultimately unifies the relevant policymaking process through a single regulatory body (the FCC) that will often act like an appellate court (albeit subject to the oversight of the D.C. Circuit) as it develops a uniform body of unfair competition law.

In short, the case for a no-delegation or limited delegation model depends on how one judges three primary factors: (1) the relative assessment of the capabilities of states or a federal agency to act with fidelity toward a competition policy jurisprudence; (2) the level of confidence in the federal or state agencies' ability to adapt to a rule of law, adjudicatory model (as opposed to the traditional legislative model); and (3) the judgment as to whether state involvement would give rise to more benefits or harms in the administration of competition policy. As noted above, the Working Group members differed on their evaluation of these factors and thus whether a no-delegation or limited delegation model would be preferable.

### *C. Consumer Protection and Social Policy*

Unlike competition policy matters, where our Working Group believes that the FCC should take the lead in establishing the governing policy framework, consumer protection and certain social policy concerns are more properly handled—at least in the first instance—by state agencies. As Commissioner Kennedy put it, "federal regulators would never be equipped to accept millions of calls from individual customers involved in billing disputes" and it makes no sense for "the FCC to assume the responsibility for addressing these and other consumer complaints at the retail level."[34] Under current practice, state agencies oversee all carriers within their jurisdiction by, among other things, requiring certification and managing numbers within the appropriate area codes. The role of certification requirements, as suggested by the

33. Again, as noted in footnote 27, we recognize that the institutional reform Working Group may well modify the procedures or institutional structure of the FCC and do not mean to indicate a preference for a particular set of reforms (or the FCC as it currently operates).

34. Kennedy, *supra* note 12, at 5.

above discussion, should be limited either to any FCC-authorized competition policy measures (under the "Limited Delegation" option) or appropriate consumer protection or other social policy concerns. Under no circumstances, however, should certification requirements be any more burdensome than absolutely necessary to accomplish such concerns, lest they become a barrier to entry.

In our view, in addition to protecting consumers from "unfair and deceptive practices" pursuant to DACA's Title I—Regulatory Framework, states should be allowed to promote public safety and homeland security, as well as manage public rights-of-way. States and localities would enjoy leeway in these areas regarding whether and how to impose any regulatory requirements. Specifically, whether or not the state or local obligations are expressly anticipated (such as a prohibition on slamming), states would be permitted, at least as an initial matter, to adopt any regulations they deemed appropriate. State authority would be curtailed, however, where the relevant obligations were inconsistent with federal law, "where there are substantial and clear efficiencies from eliminating diverse approaches, where a single approach is clearly optimal over others, or where there is a clear showing that the costs of diversity outweigh the benefits of state experimentation and implementation."[35] Similarly, where state regulations would create harmful and significant spillover effects, the FCC would be authorized (and indeed required) to preempt state regulation, thereby preventing a single state from imposing its suboptimal policy on the entire country. These "no spillover" standards are meant to remedy current holes in the Section 332 model used for wireless services, where reserving consumer protection authority to states has allowed *de facto* economic regulation in the name of consumer protection.

The decision to leave the state agencies with the initial authority to address these matters reflects the judgment that their proximity and accessibility to the affected consumers make them the superior institution to address such matters in the first instance. With respect to the consumer-affecting matters identified by the Working Group, states have adopted a range of strategies, including litigation, agency oversight, and consumer education initiatives. Following such experiments, such as the early efforts to develop a "do not call list," other states have adopted best practices and, in many cases, the federal government has embraced the best of breed and adopted similar measures as federal policy.

35. Weiser, *Cooperative Federalism and Its Challenges*, *supra* note 23, at 729.

## IV. THE ROLE OF LOCALITIES IN TELECOMMUNICATIONS REGULATION

The role of localities in telecommunications regulation is an area of longstanding controversy, particularly insofar as new technologies have not fit the mold of their established counterparts. This Part discusses four prominent issues where local authorities have influenced telecommunications policy: (1) rights-of-way (ROW) management; (2) the administration of franchise requirements; (3) municipal entry into telecommunications markets; and (4) telecommunications specific taxation. We discuss each in turn, noting our respective recommendations. In general, the Working Group recommends that authority to act in these areas be given (if at all) to state agencies, with limited delegation to local authorities.

### *A. Rights-of-Way Access and State and Local Regulation*

From the perspective of service providers, access to ROW is an essential predicate to entering a particular market and is often a gating factor. For localities, regulation of access to ROW is critical to "minimiz[ing] the damage to their expensive streets, limit[ing] traffic disruption, and, in some cases, supplement[ing] their general revenue by taxing carriers' use of [ROW]."[36] Given the importance of this issue, it is most unfortunate that, "almost nine years after the enactment of the Telecommunications Act of 1996, issues regarding access to public rights-of-way between providers and local authorities continue to be the focal point for dispute."[37]

The continuing legal disputes related to ROW issues relate both to the importance of the issue and the 1996 Act's lack of clear guidance on it. In 1996, Congress set forth a broad policy (codified in Section 253) of removing barriers to entry.[38] This broad policy contained four distinct

36. James B. Speta, *Competitive Neutrality in Right of Way Regulation: A Case Study in the Consequence of Convergence*, 35 CONN. L. REV. 763, 763 (2003).

37. Paul Glist et al., *Telecommunications "Franchising"*, 818 PLI/PAT 589, 593 (2005).

38. In its entirety, Section 253 provides:

> In general
> No State or local statute or regulation, or other State or local legal requirement, may prohibit or have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service.
>
> (b) State regulatory authority
> Nothing in this section shall affect the ability of a State to impose, on a competitively neutral basis and consistent with section 254 of this title, requirements necessary to preserve and advance universal service, protect the public safety and welfare, ensure the continued quality of telecommunications services, and safeguard the rights of consumers.

parts: (1) a call to preempt any state or local regulation that would "have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service"; (2) a safe harbor for state police power activities, including consumer protection; (3) a preservation of authority to "manage the public rights-of-way," including a right to "require fair and reasonable compensation from telecommunications providers, on a competitively neutral and nondiscriminatory basis"; and (4) FCC authority to enforce this policy. Like so much of the 1996 Act, each of these parts has spurred litigation, although many of the contested issues have yet to reach the Supreme Court.

In a stark reminder of the importance of access to ROW on reasonable terms, a recent AEI-Brookings Institute report highlighted that pro-competitive ROW policies are more significant in promoting broadband deployment than universal service policies.[39] Given the lack of legal certainty under federal law, different states have adopted different policies on the appropriate regulation of ROW. In light of the clear importance of promoting broadband deployment, however, it seems prudent to adopt a nationwide policy of reasonable access along the lines of some progressive state policies, such as California's. Under California law, governmentally imposed charges for ROW access "shall not exceed the reasonable costs of providing the service for which the fee is charged."[40]

---

> (c) State and local government authority
> Nothing in this section affects the authority of a State or local government to manage the public rights-of-way or to require fair and reasonable compensation from telecommunications providers, on a competitively neutral and nondiscriminatory basis, for use of public rights-of-way on a nondiscriminatory basis, if the compensation required is publicly disclosed by such government.
>
> (d) Preemption
> If, after notice and an opportunity for public comment, the Commission determines that a State or local government has permitted or imposed any statute, regulation, or legal requirement that violates subsection (a) or (b) of this section, the Commission shall preempt the enforcement of such statute, regulation, or legal requirement to the extent necessary to correct such violation or inconsistency.

47 U.S.C. § 253 (1996).

39. Scott Wallsten, *Broadband Penetration: An Empirical Analysis of State and Federal Policies* (AEI-Brookings Inst. Joint Ctr. on Regulatory Studies, Working Paper No. 05-12, 2005), *available at* http://aei-brookings.org/admin/authorpdfs/page.php?id=1161.

40. CAL. GOV'T CODE § 50030 (2003). In full, the California law provides:

> Any permit fee imposed by a city, including a chartered city, a county, or a city and county, for the placement, installation, repair, or upgrading of telecommunications facilities such as lines, poles, or antennas by a telephone corporation that has obtained all required authorizations to provide telecommunications services from the Public Utilities Commission and the Federal Communications Commission, shall not exceed the reasonable costs of providing the service for which the fee is

The appropriate nationwide policy on rights-of-way access should not only restrict localities and states to the imposition of any requirements necessary to legitimate rights of way management, but it should also limit the payment of fees to those related to costs caused by the effort to access rights-of-way.[41] For states and localities, it is tempting to levy fees related to, say, gross receipts in order to raise additional revenue. But such revenues constitute, in effect, a special tax on telecommunications providers and thus promise to deter the use of telecommunications services (and slow their deployment). To be sure, governmental entities highlight that ROWs are governmental property held in trust for the citizenry. This form of trust is breached, however, when governmental units take action that (unbeknownst to the citizenry) restricts the deployment of new technologies.

The various forms of communication technologies call for a broad definition of "electronic communications providers" which merit protection under the above provision. In numerous jurisdictions, providers have litigated the question of whether they fall within the class of providers entitled to reasonable ROW access. In California, for example, Williams Communications offered the following explanation, which an appeals court ultimately embraced:

> The [fiber optic] cables do one thing: they carry digitized optical signals (i.e. 1's and 0's) for customers, the content of which is neither controlled nor manipulated by Williams. Once the digital signals leave the Williams system, customers convert the signals into different forms of information, such as voice, music, video, computer data, facsimile material and other forms. Any particular cable or fiber may carry digital signals at any given time that will be converted for telephone, video, Internet and/or other forms of information. . . . Williams does not and cannot, as a matter of technology, determine the particular form of information carried on its lines at or over any given period of time.[42]

The Working Group concludes that, in calling for a reasonable access to ROW for all communications providers, it is important that states or localities not impose other barriers to entry. Consequently, the Working Group recommends that a revised version of Section 253 not

---

charged and shall not be levied for general revenue purposes.

*Id.*; s*ee also* Williams Commc'ns v. City of Riverside, 114 Cal. App.4th 642 (2003) (interpreting provision).

41. *See* Speta, *supra* note 36, at 795-802.

42. *Williams Commc'ns*, 114 Cal. App.4th at 651.

only explicitly address ROW issues, but also preempt any legal requirement that "materially inhibits effective entry."[43]

Finally, the Working Group recommends that states work cooperatively with local authorities to police consumer fraud, to promote public safety and homeland security and to manage public rights-of-way. Accordingly, the proposed legislation allows states to delegate authority to local authorities to act regarding these issues. To the extent that a state follows a "home rule" model, such delegation shall be presumed (including for issues like permitting to lay cable under municipal streets) unless otherwise provided for by the particular state. In all events, however, no certification requirement should be unnecessarily burdensome so as to constitute a barrier to entry or (as discussed below) to impose requirements such as those traditionally associated with franchises to operate particular services.

### *B. Video Franchises*

As with calling for a restricted role for governmentally imposed barriers to entry and limitations on access to rights-of-way, the Working Group expressed skepticism regarding the continued need for classic "franchises" imposed on cable television providers. In the case of telecommunications providers of different services—say, telephone service or broadband—it is clear that reasonable access and no barriers to entry is a critically important public policy. Nonetheless, some localities maintain that, even as the communications environment moves towards "everything over Internet Protocol," it is essential that the traditional cable franchise be allowed to continue. Before engaging the merits of this issue and the calls for "regulatory parity" between cable providers and telephone providers of Internet Protocol Television (or IPTV), we believe that it is important to place this issue in historical context.[44]

#### 1. The Past As Prologue?

Cable television providers were the first new entrants into the telecommunications market. Before the development of Community Antenna TV (CATV), television (and radio) broadcasters—along with local telephone companies—enjoyed a form of franchised monopolies. In the case of telephone companies, states often legislated bans on entry and localities (for extra protection) might authorize access to the rights of

---

43. In so doing, it would resolve a split between the circuits. *See* Glist et al., *supra* note 37, at 597-98.

44. For a discussion of this point, *see* Raymond L. Gifford & Kyle D. Dixon, *Progress, Freedom, and Regulatory Transcendence*, 12.7 PROGRESS & FREEDOM FOUND. PROGRESS ON POINT 1 (2005), *available at* http://www.pff.org/issues-pubs/pops/pop12.7videoservices.pdf.

way under exclusive or preferential terms. In the case of television broadcasters, the Federal Communications Commission used its control over licenses to restrict competition between broadcasters (under the so-called *Carroll* doctrine).[45]

After a period of benign neglect, regulation of cable television providers (then known as CATV) reflected a commitment to "regulatory parity" or "level playing field" concerns. In particular, federal regulators concluded that cable providers should act and look just like broadcasters. To ensure that cable providers looked like broadcasters and were not able to avoid regulatory burdens imposed upon them, the FCC imposed a number of requirements, including mandates that they originate local programs and not provide any "pay TV" services. Under the weight of these requirements, called by one commentator as "a textbook example of anti-competitive regulation,"[46] cable television providers made only minimal strides in the marketplace. Over time, however, the FCC and the courts lifted a number of these restrictions, paving the way for cable TV's impressive growth in the late 1970s and 1980s.[47]

The development of satellite television providers (ultimately through the use of "direct broadcast satellite" or DBS) spurred another round of regulatory battles and calls for regulatory parity. The FCC rejected those calls and instituted a regulatory regime that allowed new entry. In upholding that judgment, the D.C. Circuit remarked that:

> Although a regulated industry may come to regard an agency's policies as immutable elements in the background against which the industry is set, there is no need for the agency itself to confuse means with ends; when new technology permits the statutory objectives to be attained through novel means that require the alteration or abandonment of past Commission policies, the Commission may adjust its means to retail fidelity to the legislative end.

---

45. *See* Carroll Broad. Co. v. FCC, 258 F.2d 440 (D.C. Cir. 1958); Policies Regarding Detrimental Effects of Proposed New Broadcasting Stations on Existing Stations, *Report & Order*, 3 FCC Rcd. 638, ¶ 1 (1988) (abolishing *Carroll* doctrine).

46. Thomas W. Hazlett, *The Wireless Craze, The Unlimited Bandwidth Myth, the Spectrum Auction Faux Pas, and the Punchline to Ronald Coase's "Big Joke"*, 14 HARV. J.L. & TECH. 335, 419 (2001) [hereinafter *Wireless Craze*]; *see also* Stan Besen & Robert Crandall, *The Deregulation of Cable Television*, 44 LAW & CONTEMP. PROB. 77 (1981) (criticizing early regulation of cable television).

47. *See, e.g.*, Amendment of Part 76, Subpart G of the Comm'n Rules and Regulations Relative to Program Origination by Cable Television Sys., *Report & Order,* 49 F.C.C.2d 1090 (1974); FCC v. Midwest Video Corp. 440 U.S. 689 (1979) (invalidating, as beyond FCC's Title I authority, pre-Cable Act requirements for "leased access" channels and channels dedicated to "public, educational, and governmental", also known as "PEG") programming); HBO v. FCC, 567 F.2d 9 (D.C. Cir. 1977) (invalidating restrictions on pay television).

> Indeed, the Commission has long been criticized as acting primarily to preserve the status quo, thus discouraging innovative technology; when it instead seizes upon the "comprehensive powers to promote and realize the vast potentialities of radio" that Congress has conferred upon it, the Commission is to be commended rather than castigated.[48]

Following the light regulatory touch accorded to DBS in its inception, Congress and the FCC treaded lightly in imposing new obligations upon it. Ultimately, Congress did impose some of the traditional requirements on DBS (such as must carry obligations), but it did so only after the technology developed and in a manner that respected the technology's limitations.

2. The Cable Franchising Process

The process for obtaining a franchise for cable television ranged from efforts to emulate Harold Demsetz's theory of franchise regulation as "competition for a monopoly," to efforts to obtain benefits for a community through regulated mandates (reflecting Posner's theory of "taxation by regulation") to out-and-out political deals, enriching campaign coffers or the pockets of politically connected individuals.[49] In many cases, these franchises imposed forms of rate regulation on franchised monopolies, along with an array of requirements, including a mandate to carry public, educational, and governmental channels. Owing to the requirement to obtain a franchise in every municipality, one commentator estimated the total number of cable franchises as 34,000.[50]

In 1984, Congress enacted its first comprehensive legislative framework to govern cable television providers. Earlier, the FCC (under its "Title I authority") had developed an array of rules, including federal mandates for Public, Educational, and Governmental channels, many of which it later reversed or were challenged successfully in court. In

48. Nat'l Ass'n of Broad. v. FCC, 740 F.2d 1190, 1196 (D.C. Cir. 1984) (internal citations omitted).

49. For the academic descriptions of franchising as a form of controlling monopoly or as an alternative to fiscal policy, *see* Harold Demsetz, *Why Regulate Utilities?*, 11 J. L. & ECON. 55, 63 (1968); Richard A. Posner, *Taxation by Regulation*, 2 BELL J. ECON. & MGMT. SCI. 22, 41-42 (1971). For a discussion of the cable industry's earlier years, *see generally* MARK ROBICHAUX, CABLE COWBOY: JOHN MALONE AND THE RISE OF THE MODERN CABLE BUSINESS (2002).

50. Kent Lassman, *Franchising in the Local Communications Market*, 12.9 PROGRESS & FREEDOM FOUND. PROGRESS ON POINT 1 (2005), http://www.pff.org/issues-pubs/pops/pop12.9franchise.pdf.

enacting a Title VI to the Communications Acts of 1934, Congress set forth a clear framework to govern the previous squabbles related to franchising negotiations (and renewals) as well as put an end to regulating the rates of cable television providers. After its re-institution of cable rate regulation in 1992, the 1996 Act restricted the regulation of cable's rates—owing in large part to the effective entry of DBS providers under a favorable regulatory environment—and only left intact a requirement of a regulated basic package of offerings.

In 1996, Congress envisioned an alternative model for entering local video programming markets through "Open Video Systems" or OVS.[51] In theory, the OVS option provided a pathway for telephone companies to enter the video marketplace.[52] Under this mode of entry, providers could opt for FCC approval rather than a local franchise, although OVS providers were subject to some common carriage-like requirements. Nonetheless, whatever appeal that OVS offered largely dissipated when the Fifth Circuit concluded that the choice of an OVS mode of entry did not prevent the imposition of additional requirements.[53]

Over the last year or so, local telephone companies (notably, Verizon and AT&T) have outlined a strategy of delivering video programming over fiber optic networks using Internet Protocol-based technology. Dubbing their offering "IPTV" (for Internet Protocol Television), some champions of this offering maintain that it need not comply with Title VI's classic requirements for a local franchise, particularly ones relating to building out service to all portions of a community. In response, both cable companies and municipalities have insisted on a franchise as a condition of entry and lobbying battles in some state legislatures and in Congress have ensued.

### 3. A New Way Forward

In evaluating the model approach for a Digital Age Communications Act, the Working Group developed a new regulatory strategy to govern the delivery of video programming that would recognize the overall economic and technological convergence of services with other digital electronic communications services. In so doing, we recognized that the continuing rate regulation of a basic package of video

51. 47 U.S.C. § 573 (1996).

52. In the 1996 Act, Congress repealed a longstanding ban (forged from a fear of anticompetitive tactics) on telephone company entry into video markets . *See* Pub. L. 104-104, § 302(b)(1) (repealing 47 U.S.C. § 533(b)). Prior to this repeal, the courts, which originally tolerated this ban, were growing increasingly skeptical of its legality. *Compare* Gen. Tel. v. United States, 449 F.2d 846 (5th Cir. 1971) (upholding ban), *and* Chesapeake & Potomac Tel. Co. v. United States, 42 F.3d 181, 202 (4th Cir. 1996) (invalidating ban), *vacated as moot*, 516 U.S. 415 (1996).

53. *See* City of Dallas v. FCC, 165 F.3d 341, 347-48 (5th Cir. 1999).

offerings had become antiquated and that an overly cumbersome franchising process for IPTV providers represented a formidable entry barrier.[54] Consequently, we embraced a revised framework that, at a state's option, would provide for statewide certifications that would entail no rate regulation or build-out requirements.

The Working Group recommends that states and localities not be allowed to impose rights-of-way or certification requirements on providers to the extent they rely on spectrum or other non-physical means to reach customers. We determined that, in those circumstances, providers will not affect public rights-of-way sufficiently to justify such requirements. We recognize that the limitation on state authority results in disparate treatment of these providers compared with providers which deploy physical networks (e.g., optical fiber, coaxial cable) to connect their customers. Although states must retain limited authority to prevent providers relying on physical networks from disrupting roads and other public infrastructure, such need is largely absent with respect to providers relying on non-physical networks. The Working Group decided that extending regulation where it is not needed simply to promote "parity" would undermine DACA's broader goal of promoting investment and innovation by avoiding unnecessary regulation of electronic communications services.

A similar desire to avoid unnecessary regulation prompted the Working Group to preclude state or local network "build-out" requirements. In theory, build-out requirements may be a plausible strategy for ensuring universal service by a monopoly provider. For a second entrant, however, the universal access concerns are irrelevant, making such a requirement entirely redundant and a barrier to entry for areas that would warrant competition. To be sure, we recognize a plausible equity concern that the first entrant has born the added responsibility of a build out requirement (that may not be profitable) and thus some Working Group members supported a "universal service fee" for IPTV providers. The majority of the group, however, concluded that

---

54. Would-be entrants have criticized the cumbersome regulatory process at the local level, explaining that:

> [T]o anyone who has actually tried to build a competitive system, it is painfully obvious that local regulators have become the bottleneck in the system. These regulators have emerged as neighborhood tyrants, protecting existing local and regional monopolies and effectively holding competitive broadband hostage. By creating unreasonable demands on any new entrant to the market, local regulators have slowed the advancement of broadband at the very moment when the telecom industry might finally be ready to enter the new age of innovation.

David McCourt, *What's a Polite Word for "Shakedown"?*, WALL ST. J., Oct. 1, 2005, at A9. Although there are, to be sure, local regulators who have facilitated robust entry, persistent complaints from the competitive community regarding local regulators persuade the Working Group that change like that proposed here is warranted.

the historic incumbency and first mover advantages that accompanied the requirement more than offset its burdens.

With respect to the use of a certification process, the Working Group agreed that there were notable ways in which the traditional franchising obligations (such as Public, Educational, and Governmental (PEG) channels) failed to live up to their initial aspirations (or, in the views of some, were misguided from the outset). In particular, local jurisdictional control of these channels or a limited amount of creativity and flexibility led to a number of disadvantages in the form of preventing sensible regional cooperation, sharing of facilities, and uses of alternative technologies (including websites, podcasting, and other viable forms of new media). While some members of the group pressed the strategy of reforming such franchise obligations by incorporating them into a statewide oversight process, the majority converged on the plan of eliminating them altogether. In so doing, the majority suggested that, to the extent states and localities wish to support video programming, they should work collaboratively with providers to ensure that such programming is delivered to their citizens (either on a purchased or contributed basis).

The Working Group recognizes that many state and local authorities have relied on franchise terms and conditions as means of benefiting their citizens. Thus, although we eliminate these features for the above reasons, we provide a transition period to provide some time for states and localities to make other arrangements. Specifically, we require the terms of existing franchises to be honored for a reasonable period, such as 3-5 years. Further, to lessen the disparity between incumbent cable franchise and telephone companies entering the video market, we afford states discretion to allocate an equitable portion of the costs of franchise fees and public access channels on telephone companies providing video programming. Although this approach does not eliminate all disparities or distinctions based on technology, we view this transition as an appropriate accommodation for state and local reliance interests and conclude that any ill effects associated with the terms of the transition will be mitigated by its short duration.

In envisioning video franchisees in a more flexible and creative light, it is also important to ensure that they do not impede entry. By replacing the franchising process with optional certification at the statewide level, we believe that transaction costs will be limited and that entry will be expedited. Finally, in terms of the particular state institution to manage this process, we follow the precedent of the Universal Service Working Group and conclude that it should be the state public utility commission unless the State Legislature appoints a different body to do so.

### *C. Municipal Entry*

One issue that has attracted considerable heat (and often little light) over the last year is the prospect of municipalities entering into the telecommunications marketplace. In general, the Working Group is skeptical that municipalities can provide more effective services than their private sector counterparts.[55] Moreover, the Working Group also notes that, where municipalities make large scale investments, there is a possibility that they will use the police power (or taxing authority) to ensure that they are recovered.[56] Such concerns are notable, but for the reasons set forth below, we do not believe that a federal ban on municipal provision of telecommunications services—through wireless or other technologies—is appropriate.

In addressing this issue, we begin by noting that state law limitations on municipal entry raise an issue entirely separate from federal law limits. In terms of sovereignty, local municipalities rely on state law to empower them (often through a "home rule" regime). Because municipalities are creations of state law, we are mindful that efforts to protect localities against state regulation raise serious intergovernmental concerns. Consequently, we leave to the states whether or not to restrict municipal entry into telecommunications markets.

In declining to recommend legislation on this issue, we will suggest that it is quite plausible that reasonable cases of municipal entry into local telecommunications markets may exist. In particular, for local public safety applications (such as transmitting pictures of suspects in real-time), high speed access is an increasing concern. To the extent that commercial providers have not developed high speed networks to provide such functionality, a locality may well choose to contract for its construction for use by its public safety agencies. Once such a network is constructed, moreover, it may well be feasible to provide priority access to public safety and also allow the public to benefit from broadband connectivity. There may also be some sparsely populated communities unserved by commercial service providers where a municipal network may be the "last best hope" for affordable broadband access. Finally, other instances of market failure may justify municipal involvement in building broadband networks.

---

55. For a discussion of the research calling into doubt the effectiveness of municipal entry, *see* Thomas M. Lenard, *Government Entry into the Telecom Business: Are the Benefits Commensurate With the Costs?*, 11.3 PROGRESS & FREEDOM FOUND. PROGRESS ON POINT 1 (2004), http://www.pff.org /pdf/16306.pdf.

56. For a discussion of this concern, *see Anticompetitive Threats from Public Utilities: Are Small Businesses Losing Out?: Before the H. Comm. on Small Business,* 109th Cong. 12-23 (2005) (statement of Adam Peters, Research Fellow, Progress & Freedom Found.).

Stated more generally, we are wary of instituting categorical limitations on municipal development of broadband or other communications technologies until we know more about their actual usage and cost characteristics. Rather, we suggest close scrutiny of them, confident that mistaken investments will defer other foolhardy efforts, and that legal safeguards against anticompetitive conduct should be vigilantly applied where appropriate. In particular, the Working Group notes that anticompetitive behavior is a promising strategy for municipally-backed market entrants and therefore would subject them to the same "unfair competition" standard as other market players.[57]

### *D. State and Local Taxation*

The final way in which state and localities can hamper the development of electronic communications services is through industry specific taxation. With respect to taxation, we noted above that imposing costs on a particular industry—such as through excise taxes or rights-of-way fees—can deter the use of that industry's products or services. In cases where the tax is imposed on a "social bad," say, cigarettes, or even where the tax reflects a close proxy to a publicly provided resource (say, the relationship of gas to the funding of roads), deterring usage may not present a grave concern. But where the tax or fee is imposed as a means of raising general revenues, policymakers should be wary of singling out a specific industry. In the case of telecommunications, such taxes appear to be on the rise and thus are increasingly troubling.[58] For that reason, we call for preemption of all industry-specific taxation on electronic communications services.

## CONCLUSION

In conclusion, we emphasize that the Report's direction and the associated draft statutory language adhere as closely as possible to the following principles:

**Pro-competitive**—Consumer welfare-driven competition policy is the overarching theme of DACA, outlined in the Regulatory Framework, and continued in this report. In authorizing state regulation, this framework emphasizes the role of a more rigorous, robust competition policy analysis and provides a mechanism for preempting regulations that are not so justified.

---

57. David E.M. Sappington & J. Gregory Sidak, *Competition Law for State-Owned Enterprises*, 71 ANTITRUST L. J. 514 (2003); Timothy J. Muris, *Clarifying the State Action and Noerr Exemptions*, 27 HARV. J.L. & PUB. POL'Y 443 (2004).

58. Dennis Cauchon, *City, State Cell Phone Taxes on the Rise*, USA TODAY, May 8, 2005, *available at* http://www.usatoday.com/news/nation/2005-05-08-cellphone-taxes_x.htm.

**Generality**—The language aspires to be concise and general, as opposed to prosaic and prescriptive. Statutory delegations relating to a dynamic sector like communications regulation must be able to adapt to the rapidly changing circumstances, and not get bogged down in special provisions and specific carve-outs for favored (or against disfavored) entities.

**Neutrality**—The language aspires to bring all platforms and all regulatory jurisdictions within a unitary policy framework, administered by the FCC but cognizant of the states' comparative advantage in some roles.

**Practicality**—The federal/state framework recognizes the role of state regulation, its political vitality and its possible salutary purpose. The proposal recognizes traditional state roles relating to consumer protection, public safety, homeland security and management of public rights-of-way. It likewise preserves the ability to potentially retain a basic service rate, without undue distortion of the competitive market.

## APPENDIX A: MODEL PROPOSED LEGISLATIVE LANGUAGE

The Digital Age Communications Act

### Title II—ALLOCATION OF FEDERAL, STATE AND LOCAL RESPONSIBILITY

Section 1: Findings

(a) FINDINGS. The Congress finds the following:

that technological and market forces are changing the nature and delivery of electronic communications services;

that these technological and market changes have altered the necessary roles for federal, state and local authorities in regulating electronic communications services;

that, in many cases, responsibility to regulate activities relating to communications has been allocated to a state or local jurisdiction based on whether such activities were deemed to occur within that jurisdiction;

that as electronic communications services and technologies become increasingly digital and packet-based, it has become difficult, and often impossible, to rely on jurisdictional boundaries as the basis for allocating regulatory responsibility among jurisdictions;

that a regulatory regime enforced by multiple jurisdictions, based on disparate laws, may result in inconsistent, unpredictable and onerous rules that inhibit investment, innovation and competition;

that the Telecommunications Act of 1996, which made substantial changes in the allocation of responsibilities among regulators in different jurisdictions, nonetheless did not adopt a framework that addresses fully the challenges posed by the rapid technological and marketplace evolution of electronic communications networks and services; and

that given these shortcomings, new statutory guidance for allocating federal, state and local responsibility is necessary to achieve the purposes of regulating electronic communications networks and services.

(b) POLICY. In light of the findings in subsection (a), it is the

policy of the United States:

to integrate federal, state and local regulation of electronic communications networks, as developed by this and other titles of this Digital Age Communications Act;

that electronic communications networks and services be governed by a single, unified, minimally pervasive regulatory regime determined and generally implemented at the federal level;

to eliminate rate regulation and rate-setting where market conditions adequately protect consumers' interest in reasonable rates;

to eliminate regulation based on technological or functional distinctions among communications services and networks;

to avoid extending legacy regulation to additional services, networks or providers;

to create incentives to invest in new technologies and encourage the deployment of advanced electronic communications services.

Section 2: State Regulation of Basic Local Rates

(a) GRANDFATHERED RATE REGULATION. Subject to the limitations of subsection (b), (c) and (d), a state may continue to regulate the rate for a basic, stand-alone local service. To qualify as such a service, immediately prior to the date of enactment of this Digital Age Communications Act, the service must have been (and must continue to be):

(1) offered separately from any other services to customers who are not providers of electronic communications services;

(2) of the type defined in 47 U.S.C. § 254 (c)(1), as interpreted by 47 C.F.R. § 54.101(a);

(3) provided via a circuit-switched telephone network; and

(4) lawfully regulated by the state.

(b) Rate regulation authority under this section shall not extend to any ancillary or vertical services offered in connection with basic, standalone local service, or apply to any service bundles that contain basic standalone local service as a component.

(c) Neither the Federal Communications Commission nor the states shall have rate regulation authority over any other retail or end-user electronic communications service except under section 3(a) of this Title II, or as authorized under Title I, Section 3: Unfair Methods of Competition Unlawful of this Digital Age Communications Act.

(d) REFORM OF RATE REGULATION. Parties at any time may petition a state authority to modify or eliminate its regulation of rates that otherwise would be preserved pursuant to subsection (a).

(1) The state authority receiving such a petition shall issue an order disposing of the petition within 270 days of receiving the petition or it will be deemed granted. For every service for which a state determines to continue to regulate the rate, the order shall demonstrate that the rate meets the qualifications of subsections (a) and (b) and (c) and shall also explain why the economic benefits of such regulation (or non-regulation) outweigh its economic harms.

(2) Parties may petition the Federal Communications Commission to review aspects of proceedings conducted pursuant to subsection (d)(1), including petitions to modify or eliminate rate regulation that are deemed denied.

(3) Within 180 days of receiving such a petition, the Federal Communications Commission shall issue an order preempting regulation of any rates that do not remedy methods or practices deemed unlawful pursuant to Title I, Section 3: Unfair Methods of Competition Unlawful. If the Commission fails to act within 180 days of receiving such a petition, it will be deemed denied.

(4) Parties may appeal the grant or denial of a petition pursuant to subsections (d)(2) and (d)(3) to the United States Court of Appeals for the District of Columbia Circuit.

Section 3: Implementation of Title I, Regulatory Framework

*[No Delegation Option]**

(a)*The Federal Communications Commission shall be the sole agency with jurisdiction to implement regulation and conduct adjudications under Title I-Regulatory Framework, except as specified in Section 4: State and Local Regulation.*

(b)*The Federal Communications Commission may not delegate authority to states to promote competition among providers of electronic communications services.*

*[Limited Delegation Option]***

(a) **COMMISSION-INITIATED DELEGATIONS. Except as expressly provided in Sections 2, 3(b) and 4 of this Title, the Federal Communications Commission shall have exclusive jurisdiction and authority to enact or implement rules, regulations or obligations, or conduct rulemakings or adjudications, under Title I-Regulatory Framework.**

(b)**For matters occurring wholly within a given state or locality, the Federal Communications Commission may delegate to that state or a subdivision thereof the authority to enforce any rules, regulations or obligations enacted or determined by the Federal Communications Commission under Title I – Regulatory Framework, or adjudicate disputes between providers of electronic communications services that implicate such rules, regulations or obligations.**

(1) **A delegation of authority pursuant to subsection (b) will be deemed invalid if the state or locality does not certify, and the Federal Communications Commission does not concur, that the state or locality is legally and practically competent to implement the action the Commission seeks to delegate. Such determinations will not be subject to collateral attack or interlocutory appeal.**

(2) **If a state or locality declines to accept, lacks authority or otherwise fails to implement a delegation of authority pursuant to subsection (c), upon public notice, the Federal Communications Commission shall assume responsibility for implementing that delegation.**

(3) **A state or locality may petition the Federal

> Communications Commission to clarify the scope of a delegation of authority pursuant to subsection (c) or to obtain a waiver from any express or implied limitations on such delegation. Within 120 days of receiving such a petition, after affording interested parties the opportunity for comment, the Federal Communications Commission shall issue an order granting or denying the petition or it will be deemed granted.

(c) **Parties may appeal all decisions of the Federal Communications Commission or any state or subdivision thereof, as applicable, arising from this Section to the United States Court of Appeals for the District of Columbia Circuit.**

(d) **PETITIONS FOR DELEGATION. In the absence of delegated authority pursuant to subsection (b), a state or locality seeking to impose obligations among providers of electronic communications services under Title I, Regulatory Framework must petition the Federal Communications Commission for approval or denial of the proposed obligations.**

(1) **Within 90 days of receiving such a petition, the Federal Communications Commission shall issue an order granting or denying such petition or it will be deemed denied. Such determinations will not be subject to collateral attack or interlocutory appeal.**

(2) **After an appropriate notice and comment in response to a petition by any party—or on its own motion—the Federal Communications Commission may preempt actions taken in response to the granted petition, provided the Commission satisfies the requirements of Section 5: Limitations on State and Local Authority.**

(3) **State or localities may only petition under this subsection (d) as to matters contained and confined wholly within the petitioner's jurisdictional boundary.**

Section 4: State and Local Regulation

(a) AUTHORITY OF STATES. Notwithstanding Section 3, and subject to Section 5 of this Title, states or subdivisions thereof retain jurisdiction to enact and implement rules or regulations that the state or

subdivision thereof determines, after notice and an opportunity for public comment, are minimally and directly necessary to:

(1) Prohibit unfair or deceptive acts or practices that would negatively affect consumers from using electronic communications services, including, by way of example, concealment of the terms and conditions affecting the price and quality of such services;

(2) Protect public safety and homeland security;

(3) Manage public rights-of-way and execute traditional police powers with respect to public spaces, provided that any fees imposed for access to rights-of-way shall not exceed the actual direct costs incurred by the state or subdivision thereof in managing the electronic communications service provider's use of such rights-of-way.

(b) SCOPE OF STATE AUTHORITY. Nothing in subsection (a) should be interpreted to otherwise allow states or localities:

(1) to implement Title I—Regulatory Framework;

(2) to enact forms of rate, quality-of-service or other forms of economic regulation except as expressly permitted under this Title; or

(3) to impose requirements pursuant to subsection (a) on providers of electronic communications services to the extent they rely on networks that connect to customers primarily through use of electromagnetic spectrum or other non-physical means.

(c) CERTIFICATION AND RIGHT-OF-WAY AUTHORIZATION. Providers of electronic communications services shall be authorized to construct or operate an electronic communications network over public rights-of-way, and through easements within the state, except that in using such easements the provider of electronic communications services shall ensure –

(1) that the safety, functioning and appearance of the property and the convenience and the safety of other persons not be adversely affected by the installation or construction of

facilities necessary for the electronic communications network;

(2) that the cost of the installation, construction, operation or removal of such facilities be borne by the provider of electronic communications services or subscriber or a combination of both; and

(3) that the owner of the property be justly compensated by the provider of electronic communications services for any damages caused by the installation, construction, operation or removal of such facilities by the provider, provided that a state or subdivision thereof shall not impose fees in excess of the costs not already covered under subsection (a)(3).

(4) any provider may petition the Federal Communications Commission for review of a state's or a locality's determinations under this section (c) pursuant to Section 5: Limitations on State and Local Authority.

(d) AUTHORITY OF LOCALITIES.

(1) Any locality that provides electronic communications services is subject to Title I, Section 3: Unfair Methods of Competition Unlawful.

(e) TRANSITION AND SUNSET FOR EXISTING AGREEMENTS.

(1) Providers of electronic communications services that, according to state law as of the date of enactment of this Digital Age Communications Act, remain bound by existing agreements adopted pursuant to section 47 U.S.C. §541 shall satisfy all terms and conditions of such agreements for 4 years from the date of enactment, whichever is later.

(2) States and localities may not renew, extend or otherwise subject any provider of electronic communications services to the agreements described in subsection (e)(1) beyond the duration specified in that subsection.

(3) Until the termination of an existing franchise agreement pursuant to subsection (e)(1), states may require any

provider of competing video service that may be certificated pursuant to subsection (b) to contribute an equitable portion of the costs associated with any fees and public access channels directly attributable to the agreement.

Section 5: Limitations on State and Local Authority

LIMITATION. Notwithstanding the provisions of Sections 3 and 4 of this Title, state and local authorities are hereby preempted and thus without authority to regulate electronic communications services or networks whenever the Federal Communications Commission concludes that

(1) state or local such regulation would be inconsistent with federal law;

(2) there are substantial and clear efficiencies from eliminating diverse regulatory approaches;

(3) a single regulatory approach is clearly optimal over others;

(4) there is a clear showing that the costs of diverse regulatory approaches outweigh the benefits of state and local experimentation and implementation;

(5) a single regulatory approach is clearly optimal over others;

(6) materially inhibits any provider (other than a state or locality) from effectively offering an electronic communications service;

(7) state or local such regulation would be inconsistent with the policy goals articulated in Section 1(b) of this Title; or

(8) state or local authorities have imposed a tax solely on some or all providers of electronic communications services.

PREEMPTION. If, after notice and an opportunity for public comment, the Federal Communications Commission determines that a state or local authority has imposed any statute, regulation or legal requirement that violates subsection (a), the Commission shall preempt the enforcement of such statute, regulation or legal requirement to the extent necessary to correct such violation or inconsistency. Where the

Commission reviews a state or local statute, regulation or legal requirement in response to a petition for preemption, rather than on its own motion, it shall grant or deny the petition within 180 days of receiving it, or it will be deemed denied. Parties may appeal the grant or denial of such a petition to the United States Court of Appeals for the District of Columbia Circuit.

# WITHER THE STATES? COMMENTS ON THE DACA FEDERAL-STATE FRAMEWORK

PAUL TESKE*



## INTRODUCTION

When I started writing my doctoral dissertation 20 years ago on the topic of American state telecommunications regulation, I was not confident that my subject would outlive my study.[1] Like a former colleague who was one of the world's experts on East German national politics, I feared that my attentions would have to move on to a subject with more staying power.

So, I am surprised that state-level regulation still exists in 2006, indeed that it shows signs of having an even longer life. Given that state telecommunications regulation is unlikely to disappear anytime soon and the substantial changes in the telecommunications landscape since the federal government's last major foray into this topic, the Telecommunications Act of 1996 (1996 Act), the Digital Age Communications Act (DACA) project rightly proposes a more narrowly defined role for state regulation and policy in the future.[2] The DACA

* Professor of Public Affairs, Graduate School of Public Affairs, University of Colorado at Denver and Health Sciences Center.

1. *See* PAUL TESKE, AFTER DIVESTITURE: THE POLITICAL ECONOMY OF STATE TELECOMMUNICATIONS REGULATION (1990).

2. Kyle D. Dixon & Philip J. Weiser, *A Digital Age Communications Act Paradigm for Federal-State Relations*, 4 J. ON TELECOMM. & HIGH TECH L. 321 (2006).

report takes an incisive, but not too radical, step in calling for a changed relationship between the Federal Communications Commission ("FCC") and state regulators, one that retains some flexibility for the states, but within a much more proscribed range. I agree that a diminished role for the states is appropriate. State-level regulation used to look more attractive because it created a more flexible forum for experimenting with novel policy solutions, even as it imposed some costly jurisdictional externalities and coordination concerns. However, these benefits of state-level regulation are diminished compared to ten years ago, even as the costs might have been diminished somewhat as well.

It is clear, at least in general terms, that America has been moving for many years towards a new telecommunications regulatory model, one that relies mainly upon open competition. Abstract models of perfect competition or complete monopoly produce well-understood and predictable outcomes. The economic in-between of partial competition that has characterized the telecommunications industry over the past 20 years is much harder to understand and does not lend itself to clear policy guidance. Given that the technology advances so rapidly, most analysts advocate a policy of fairly minimal regulation. They support oversight that is based more upon industry consolidation and actual firm practices in the marketplace than upon pre-determining which firms can enter which markets and charge what prices. As the DACA authors point out, this is more like an antitrust model, and more of a federally-driven framework for regulation. Thus, the more narrow state policy role advocated by the DACA authors is appropriate.

In the next section, I demonstrate how recent trends in the state-federal relationship in telecommunications have been shaped by politics and history, as much as by academic theories. Then, I show how analysts of telecommunications federalism can learn from the history of other regulated sectors that involve both federal policy and state implementation. In the fourth section, I assess in more detail the specific DACA proposals for the remaining state role. Finally, I conclude with some expectations about how the state role can be changed further in the future.

## I. TELECOMMUNICATIONS REGULATORY POLITICS, POLICY, AND FEDERALISM

In retrospect, perhaps much of my worry about the states' role disappearing was naïve. In subsequent research, I have become very much aware that intra-industry politics play an enormous role in determining whether federal or state regulators will hold sway over some parts of an industry. If powerful interests gain from state regulation, and want to keep it as part of the overall regulatory framework, state

regulation is likely to remain in place, even in the face of evidence that it is not beneficial. In reality, this political power tends to trump grand and well-meaning academic theories of federal-state jurisdictional authority. Thus, politics and positive theory shapes jurisdictional questions as much or more than pure normative theory.[3] Certainly, even U.S. Supreme Court decisions rarely seem consistent on broad questions of federalism and national power, but appear to vary based upon the outcome hoped for by a majority of the jurists on a particular policy.[4] Indeed, the "D2" combination of "Deregulation and Devolution" within the regulatory policy sphere has not always met the conservative policy goal of a smaller role for government involvement in the economy.

In telecommunications, some would argue that state regulation has served the interests of the major regulated incumbent firms, the former Baby Bells, quite well since divestiture.[5] This is especially true since a few other them – SBC/AT&T (now merged, called "AT&T" again, and poised to merge with Bellsouth too), and Verizon in particular – are the strongest survivors of the industry battles of the last two decades and the two largest landline forces in the industry today. So, whether or not the state role will change substantially will depend partially upon how firms like these view their future prospects at the state versus the federal levels of regulation.

I have also observed the incredible "stickiness" of state regulation in a number of industry domains. State regulatory structures can remain in place years after their demonstrated value to anyone save for the most narrowly focused rent-seekers. For instance, state economic regulation of the trucking industry remained in about half the states for 15 years after the 1980 federal deregulation of interstate trucking regulation, until Congress finally preempted it out of business.[6]

And, looking beyond the trends in state telecommunications regulation, the whole arena of state regulation generally appears to be experiencing an upsurge. New York State Attorney General Eliot Spitzer has been at the forefront of renewed state enforcement actions in antitrust and financial regulation. More generally, the states have stepped up to play a more forceful balancing and "re-enforcement" role, in response to a federal government that has accelerated deregulation and "de-enforcement," perhaps even more than a clear majority of citizens

3. AMERICAN REGULATORY FEDERALISM AND TELECOMMUNICATIONS INFRASTRUCTURE (Paul Teske ed., 1995).

4. JEFFREY SEGAL ET AL., THE SUPREME COURT IN THE AMERICAN LEGAL SYSTEM (2005).

5. *See, e.g.*, John Dunbar, Former Bells Dial up Big Numbers in Statehouses (Sept. 29, 2005), http://www.publicintegrity.org/telecom/report.aspx?aid=744.

6. Paul Teske et al., *Federal Preemption and State Regulation of Transportation and Telecommunications*, 23 PUBLIUS 71, 78 (1993).

have wanted.[7]

But, it is also true and important that telecommunications is somewhat different and distinct from other areas of regulation. Many other industries could make an argument about the declining importance of what might be considered to be truly "intra state commerce" in their field, (e.g., insurance), suggesting that the role of states as central regulators of these activities should also be waning. However, the argument is even stronger for telecommunications, particularly given the industry's central role in this country's present and future economy. As the DACA report notes, it is now commonplace to point out that in the "digital age" of packet-switched, Internet protocol technology, standard spatial geography is increasingly irrelevant. Whether states should continue to make important regulatory decisions when the technology is flying way over their heads is a reasonable question to ask. This point is also demonstrated effectively in the challenges that states have faced in trying to figure out a fair and efficient mechanism for sales taxation of Internet purchases that are made in many taxing jurisdictions.[8]

Stacked against these compelling arguments for a diminished state role is the tradition of states as experimental laboratories for novel regulatory approaches. Such policies can be more easily adopted, imitated, or discarded than at the federal level. This has not been a trivial theoretical point in telecommunications. Many of the competitive ideas in the 1996 Act came from experimental evidence gathered in states like New York, Nebraska, Illinois, California, and others. But, given the rapid changes in competition within the industry, it is harder and harder to see the advantages of the experimental element of state regulation, while the slow speed and patchwork nature of multiple state oversight have become more apparent; indeed, it prompted this DACA project. While greater responsiveness to a more homogeneous group of consumers and firms has been offered in support of continuing state regulation, this also makes less sense in a competitive industry where consumer needs seem fairly similar across states.

## II. TELECOMMUNICATIONS REGULATION COMPARED TO OTHER INDUSTRIES

Having already argued that telecommunications is somewhat distinctive, I do not want to belabor comparisons to other industries too much. Still, we can learn more about how and when state regulation can

7. *See* Paul Teske, *Checks, Balances, and Thresholds: State Regulatory Re-enforcement and Federal Preemption*, 38 PS: POL. SCI. & POL. 367 (2005).

8. Samuel J. Best & Paul Teske, *Explaining State Internet Sales Taxation: New Economy, Old-Fashioned Interest Group Politics*, 2 ST. POL. & POL'Y Q. 37-51 (Spring 2002).

play a useful role by assessing it in the context of other industries to gain a broader historical perspective. The federal government has not yet deregulated interstate telecommunications completely; indeed it took 15 years for total state preemption after the federal trucking industry was deregulated. With the specter of a similar lag time, it may not yet be time for state preemption of telecommunications regulation, politically and historically. Given the importance of telecommunications to our present and future economy, a stronger argument can be made for slower, more careful, and more incremental decision-making when compared to full and immediate deregulation.

Railroads were the first major industry that involved not only regulatory questions, but explicit federalism issues, starting in the 1870s. After interesting jurisdictional battles and questions about how much any level of government could actually regulate within Constitutional boundaries, the 1887 Interstate Commerce Act developed a hybrid federal-state framework.[9] But, actual railroad shipping movements very quickly became largely interstate in nature. Many early 20th century legal cases gave prominence to federal regulation in this industry. Truly intrastate railroad carriage became a small part of freight delivery 100 years ago. Thus, intrastate regulation, faded from importance since the substantive domain over which it ruled was a quite small marketplace. By the time state economic regulation of the railroad industry was preempted in the 1980 Act (at the same time federal economic regulation was also largely deregulated), it simply was not that important to anyone any more.[10] Thus, one lesson is that state regulation can be ceased fairly easily when it has already gradually faded away in substantive terms.

The pattern was different in trucking regulation, where delivery of most shipments was truly intrastate in nature. And, historically, trucking industry regulation had developed initially from the states up to the federal level, much more so than with the railroads. When federal economic regulation of trucking was substantially deregulated in 1980, the same year as railroad deregulation, the states were not preempted.[11] This was partly because of more intrastate activity in trucking, more state interest in maintaining regulation, and other necessary Congressional compromises to achieve passage of this legislation.[12] While several states chose, on their own, to deregulate after 1980, about half the states still had some important economic regulation in place in 1994. The states

9. *See* Eli Noam, *The Federal-State Friction Built into the 1934 Act*, *in* AMERICAN REGULATORY FEDERALISM AND TELECOMMUNICATIONS INFRASTRUCTURE 113 (Paul Teske ed., 1995).

10. *See* PAUL TESKE ET AL., DEREGULATING FREIGHT TRANSPORTATION: DELIVERING THE GOODS (1995).

11. *Id.*

12. *Id.*

were only preempted by Congress in 1994, when the United Parcel Service, Federal Express, and other major firms with growing interests in trucking decided to spend considerable lobbying money and capital to make the state economic role disappear. Thus, state economic regulation of trucking stayed around in half of the country for 15 years after the federal government had deregulated and very clear and strong evidence demonstrated the advantages to deregulation. Due to narrow, but strong entrenched rent-seeking interest groups, these states had to be forced out of part of the regulatory business. It is also important to remember that states still retain important, non-economic roles in regulating trucking heights and weights, driving time restrictions, and hazardous materials routing.

Electricity regulation has also followed the state-federal, intra/interstate pattern for many decades. Federal legislation and Federal Energy Regulatory Commission actions in the 1990s encouraged the states to deregulate partially, but did not force them to do so. Again, about half the states chose to adopt a deregulatory framework, though the details of such deregulation have varied substantially across states. Before many states got too far with actual deregulatory implementation, however, the California blackouts of 2001 led to questions about the desirability of further deregulatory implementation, which has generally stalled since then. Consumers largely do not have effective retail electricity choices, even as wholesale competition has taken hold in the industry. Due to such lack of competition, and the new politics surrounding it, state regulation remains a strong force in electricity.

The insurance industry illustrates yet another iteration of federal-state regulation. The federal government does not have any important regulatory role, because insurance was not even considered to be "commerce" by the courts until recent decades, and now is regulated by a patchwork of 50 states, who sometimes work together to share information and oversight.[13] Insurance appears ripe for federal regulation to take a greater role, but historical path dependence may prove difficult to overcome, demonstrating how critical it can be in regulatory models, compared to theoretical models of jurisdictional responsibility.[14]

These industry comparisons yield several interesting conclusions. State telecommunications regulation may have lost much of its critical role, but may not be poised to fade away yet. Further, telecommunications as an economic infrastructure is much more important for most of these other industries. Rather than immediate deregulation, incremental reduction in regulation allows policymakers to

13. *See* PAUL TESKE, REGULATION IN THE STATES 97-108 (2004).

14. *See* DOUGLASS NORTH, INSTITUTIONS, INSTITUTIONAL LEARNING, AND ECONOMIC PERFORMANCE (1990).

move with more certainty in the appropriate directions and more easily reverse direction, if necessary. Giving consumers time to adjust to new market realities, especially older consumers still locked-in to older technologies and older assumptions about how regulation might protect their interests, might make sense.

## III. ADDRESSING THE DACA PROPOSALS

The DACA state-federal report addresses the two general alternatives of: (1) preempting the states completely, or (2) maintaining some minimal role for them. I agree with the DACA authors in focusing more attention upon the latter option, which comprises a more politically feasible and appropriate policy choice in 2006. The report then examines how to develop an integrated regime for regulating rates, competition, and consumer protection. Next, it turns to local and state issues, such as use of rights-of-way, video franchising rules, municipal entry, and taxation. I will address most, but not all, of these issues in the order of their presentation.

### *A. The State Regulatory Role*

In considering the appropriate future role of the states, the report suggests that the decision concerning how much authority to delegate to states depends substantially upon judgments about comparative institutional competence and the ability to manage critical tasks. Part of that management involves the ability to make relatively objective decisions based upon evidence, which can be clouded by intense political pressure to regulate in a manner that favors some groups over others.

Such political pressure is probably more balanced and provides more pluralistic "rent-seeking activity" at the federal level, compared to more unbalanced political input at the state level. Rent-seeking activity cannot and will not be curtailed, so it is worth examining as a fact of life. Still, despite the relatively less balanced interest group pressure at the state level, econometric evidence suggests that state level rent-seeking and capture are not as egregious as some would suggest.[15] Powerful groups often get favorable treatment from state regulatory processes, but the disparities are not as extreme as some appear to suspect, when they characterize state regulation as a "race to the bottom" that inevitably favors the most powerful.

State public utility commissions (PUCs) already spend a great deal of time engaging in appropriate and successful adjudicatory decisions in their normal daily activities. Because they are not exclusively rulemaking

15. *See* TESKE, *supra* note 13, at 195-200.

entities, and PUCs should manage a shift to a more "ex post" adjudication model reasonably easily. I believe that state PUC staffs are already more comfortable with this activity than the DACA report anticipates. Furthermore, state regulators and staffs have seen this writing on the wall for several years now, and all but the most stubborn will realize that a new era has dawned, and that their role, if there is to be one at all, needs to be different. Most states are ready to take on this new challenge.

There are some existing federal-state models of limited state flexibility under a general federal framework. The DACA report makes comparisons to the "cooperative federalism" mechanism of Medicaid waivers, as a process of state implementation based upon federal standards. While this provides a valuable conceptual lens, within the regulatory sphere there are even closer models of cooperation that are worth more attention. For example, the federal Environmental Protection Administration (EPA) and Occupational Health and Safety Administration (OSHA) set minimum federal standards for a number of regulated activities. States can choose to be the implementing authorities, using a state environmental or OSHA-like agency, or they can decide to let the federal government's regional offices implement policy within their state.[16] Such implementation is guided by a range of standards but usually includes some flexibility to match local conditions and problems. In addition, for environmental or worker safety issues not explicitly addressed by the EPA or OSHA, and particularly for those with a larger intrastate dimension, state agencies can experiment with other regulatory approaches beyond the federal framework. Thus, an integrated model in which state PUCs play a role akin to the role of state environmental agencies play relative to the EPA is certainly not without precedent in regulation. Historical path dependence represents a main difference that might actually influence implementation. The PUCs pre-dated the FCC, while the state environmental and worker safety agencies were largely created, or absorbed, at the same time as the EPA and OSHA were created.

In addition to these comparative elements of federal and state institutional competence and capacity, it is worth noting the wide variations across the states. The "horizontal" management capacities of PUCs across the 50 states may vary as much as the "vertical" difference between the FCC and the average state PUC. Even if the staff size of a state PUC is a function of the number of consumers it must protect, there are large differences between states like California and New York versus Wyoming and Maine. This is likely to influence the capacity to

16. *See id.* at 89-96.

make general regulatory policy, if there is a size threshold or an economies of scale element to policy development. This variable potential for non-uniform PUC regulatory practices argues for a more mechanical enforcement role for the states, as an arm of the FCC, but with some flexibility to respond to more localized consumer concerns. The concept of minimal state rate regulation, perhaps only over basic local rates, makes sense in this context.

To present an argument for re-regulation, the DACA authors address the question of whether conditions might change in the future. By definition, the case for re-regulation is not easy to imagine, but it is possible if local rates shoot up. After deregulation in 1984, cable television rates increased greatly in the late 1980s, after which Congress responded in 1992 with a form of re-regulation, even undertaking their only override of then President Bush's veto.[17] Though rate re-regulation is difficult and faces a high hurdle, this is probably the correct threshold at this point in the industry's competitive development. Or, if "unfair competition" emerges, the report notes that "ex post" regulatory mechanisms are available to address that problem, generally through federal antitrust enforcement actions.

While minimal rate regulation makes sense, I worry more than the DACA authors that the telecommunications consumer market is highly segmented and that some groups face problematic information asymmetries. The non-technology savvy consumers, which may include older, low-income, and other American groups, probably do not view cellular, VOIP, WiFi, CATV, or other communications alternatives as substitutes for their basic landline telephony, if they are even aware of them at all. Their basic rates could then rise, absent continuing rate regulation, and they would not necessarily seek alternative competitors' services. There is probably some ceiling price on this consumer inertia, but it might be a higher price than many would view as appropriate. Justifications of the price deregulation under the 1984 Cable Act included a "relevant markets" argument about regular TV, VCRs, movies at theaters, etc. were partial entertainment substitutes for cable, but unregulated cable rates still increased after the legislation was passed.[18] Again, rather than immediate rate deregulation for basic local rates, the more moderate DACA proposal seems appropriate, with a more gradual phase-out of regulation of the basic local rate, especially as some of these rates are probably still below cost in some areas. This does not, however,

17. Thomas Hazlett, *Prices and Outputs under Cable TV Reregulation*, 12 J. REG. ECON. 173 (1997).

18. ROBERT CRANDALL & HAROLD FURCHTGOTT-ROCH, CABLE TV: REGULATION OR COMPETITION? (1996).

justify more aggressive, continuing rate regulation apart from basic rates. But it does raise one area of concern under the report's category of "social policy."

### *B. State "Social Policy"*

In addressing "social policy," the DACA authors make an important distinction between economic and regulatory concerns versus other policy concerns in telecommunications regulation. I fear, however, that the term "social policy" is a poor choice for the concepts of interest. "Social policy" implies a focus upon welfare, equity, and related values, when the actual issues are consumer protection, firms' access to rights-of-way, antitrust policy, and homeland security. Even as they are somewhat distinct from economic regulation of price and competition, they do not seem to all fit under an umbrella term like "social policy." I would call them consumer and other protection issues. Calling them social policy also labels them in a certain way, pejorative for some observers, who would argue that "social policy" should be pursued through more direct subsidy means, rather than through any industry-specific policies or regulations.

Consumer protection also relates to antitrust law, which is very much the type of framework advanced quite explicitly in the DACA report. And, I agree that this is generally appropriate. It is also worth noting that an antitrust focus is also likely to be mainly a federal focus. Generally, state antitrust efforts are not supported in the report. Many analysts have supported a national, unified antitrust policy.[19] But, it is undeniable that state attorneys general, like Spitzer, have used enforcement more than federal officials in recent years, and perhaps more appropriately in some cases. Many state attorney generals argue that states have a legitimate role to play in some antitrust issues, and the question is whether and how their role in telecommunications antitrust might be affected by this proposal. By proposing an FTC-like model, I believe the DACA argues for no state antitrust activity in this area. However, I would like to see a clearer argument from the DACA authors about whether the states would retain any antitrust role in this framework.

Another issue not addressed in the report is whether or not "rent-seeking" in the adjudicatory world has some problems that could bias outcomes. More "legal" forms of rent-seeking may be less problematic than in the world of regulatory rulemaking, but they are also probably not trivial. In other words, interested parties with deep pockets may be

19. See Robert Hahn, *Federalism in Antitrust*, 26 HARV. J. L. & PUB. POL'Y 878 (2003).

more likely to bring lawsuits and complaints to policy makers, hoping to win in some cases and perhaps forestall or freeze competitors in other cases. Especially under a regime where more frivolous suits could be dismissed easily and thus would not hold up the further development of competition, this would be a more minimal concern than legislative and agency rule-making types of rent-seeking. But, it certainly does beg the question of whether residential consumers would likely pursue what they might perceive as long and difficult adjudicatory processes to address market-power or competitive abuse questions, when they know of high barriers to entry to operating successfully in that process. At a minimum, in this adjudicatory role, both state PUCs and the FCC must recognize this concern.

Overall, in terms of rates, competition, and consumer protection regulation, it seems clear that the value of state experimentation is unquestionably less than it was in the recent past. I believe that most analysts seem to agree on a general model of relying mainly upon telecommunications competition to police the American marketplace wherever possible – they do not necessarily agree on all of the details, but on the basic goal and how to get there in a general way. So, both the costs and the benefits of state regulation appear to be less than they used to be a few years ago. State regulation is just less important on both sides of the coin. That may also be true of federal regulation, though the magnitude of impacts seem larger there. So, despite the handful of concerns I raised here, I agree with the DACA report's focus on a reduced and more narrowly prescribed state regulatory role.

### *C. Other State and Local Policy Roles*

In addition to these direct regulatory questions of rates, competition, and consumer protection, a number of issues arose out of ambiguities in the 1996 Act which turn out to affect competition and telecommunications policy at both the state and local levels.[20] The DACA report is careful to address these as well, a few of which play out at the municipal level, and I add a few additional perspectives here.

In considering local issues in telecommunications, the DACA authors appropriately treat localities as "creatures of the state." Access to and usage of rights-of-way (ROW) are some of the most important local issues in telecommunications. Local governments have sought to increase their revenues by charging higher than direct costs to firms for access to ROWs. The report would limit these revenues to actual costs, but since "actual costs" remain a potential murky area, I would encourage

20. Paul Teske & Andrey Kuljiev, *Federalism, Preemption, and Implementation of the 1996 Telecommunications Act*, 30 PUBLIUS 53 (2000).

states PUCs to develop a range of acceptable costs, based upon population density, usage, weather, and other engineering-related factors. In my experience, even if ROW payments are limited to economic costs, some localities will try to justify excessive cost calculations, a problem that could be mitigated by clear state guidelines.

Another important and controversial local telecommunications issue in recent years is municipal entry into wireless broadband services. Some cities have perceived that their local providers have moved too slowly to provide this service, and have sought to provide the service themselves. In turn, telecommunications firms have pressured some state legislatures to ban municipal entry or require taxpayer votes before cities develop such services. The concerns, generally, are that municipalities may waste taxpayer funds with inappropriate technology investments and that municipalities will become incumbent firms themselves. Should they become incumbents, they will have an incentive to limit other competitors. Rather than states placing legislative limits on this activity, my own preference is to allow local voters to address the first issue, directly or through representative democracy, and to allow competitive requirements to solve the second issue.

At both the state and local level, the DACA report also indicates concerns about "regulation-as-taxation," and makes some points about direct taxation, as well. Telecommunications bills are increasingly made up of a series of taxes, fees, and charges (Subscriber Line Charges, access, etc.) that most consumers do not understand. Electric utilities and telephone companies have long been major, indirect tax collectors for state and local governments, and now cellular phone firms have also fallen into that category. While indirect taxation is not always transparent to those who pay the tax, it has some advantages in terms of being less objectionable (part of the costs of doing business) and it gets closer to a "user fee" structure that consumers can avoid if they choose.

Transparency is always a preferred public policy goal and a first-best solution to taxation issues. However, we already have a complicated system of cross-subsidies, hidden taxes, and obscured fees in telecommunications, so it is not the case that we are starting from scratch and can simply apply abstract principles. E-Rate, universal service, and other socially-oriented subsidies have some advantages, but they might not survive some types of cost/benefit assessments. They might also fall victim to political pressure in a more transparent environment. Hopefully, advancing technology, greater consumer learning, and falling costs will help minimize the need for any hidden taxes and subsidies in a more competitive environment.

Thus, while the DACA report mostly focuses upon the appropriate mix of federal regulation and state authority within a largely federal

framework, it also addresses other policy issues besides regulation. The report is consistent in emphasizing competitively-neutral solutions, where possible.

## CONCLUSION

For many years after 1984, thoughtful analysts of American telecommunications policy bemoaned the lack of specific legislative guidance to address the important regulatory and other policy issues in this critical industry.[21] A single unelected federal official, Judge Greene, oversaw the Modified Final Judgment implementation and other issues that emerged from AT&T's divestiture for more than a decade, while the FCC and state PUCs tried to develop new detailed competitive policies in a rapidly changing environment.[22] Many saw the 1996 Act as a crucial statement of legislative priorities that would help guide regulatory and other policy concerns toward an inevitably competitive industry. The Act settled some issues, but many others emerged as Internet, wireless, and advanced video technologies expanded our notions of telecommunications well beyond traditional telephone regulatory models.

We have now experienced a decade of policy implementation under the guidelines of the 1996 Act. It seems clear that a new guiding document is necessary to more fully resolve many issues, including the role of federal and state policy makers in telecommunications. The DACA report takes a crucial step in calling for a changed relationship between the FCC and state regulators, one that retains some flexibility for the states, but in a much more narrow range. Given that the advantages of state experimentation are undervalued in today's more competitive environment, it is time for a diminished role for the states. But, it is not yet time for the states to have no role in telecommunications policy. The DACA report has properly threaded this needle on most of these critical questions.

If the DACA recommendations are implemented, a period of at least a few years will be required to observe the success of the model. If local residential rates do not rise too much or too quickly, competition expands, and consumer protections remain in place, it will be time to consider whether ongoing state economic regulation will be needed at all. Then, perhaps, if it no longer seems to matter much, the state role can finally fade away.

---

21. *See generally* Teske, *supra* note 7.
22. *See* TESKE, *supra* note 10.

# TELECOM REGULATION FOR THE 21ST CENTURY: AVOIDING GRIDLOCK, ADAPTING TO CHANGE

ROBERT C. ATKINSON*



* Director of Policy Research, Columbia Institute for Tele-Information (CITI). While the views expressed herein are those of the author, he would like to acknowledge the contribution of the experts on the CITI Advisory Committee who provided guidance on the 2003 recommendations and the staff of the Journal of Telecommunications and High Technology Law, particularly Todd Hoy, Patrick Haines, Sania Anwar and Andrew Hogle for their assistance in this latest update.

## INTRODUCTION[1]

Is the regulatory system established by the Communications Act of 1934, as amended by the Telecommunications Act of 1996, suitable for the 21st century? There seems to be a growing consensus that it is not, and that "something must be done." Bills have been introduced in Congress and hearings will be held in the 2006 session.

A major reason for the current dissatisfaction with the existing regulatory system is that the 1996 amendments were obsolete when they were enacted. Because the 1996 Act was a backward-looking attempt to fix problems that had become apparent in the decade from 1985-95, it did not (and realistically could not) foresee the challenges that have resulted since 1996. These include the effects of the rapid evolution of the Internet and broadband communications, the displacement of wireline telephones by wireless, the convergence of telecom and television, and the boom-bust-consolidation of the industry.

Just as the Congress of 1995-96 was unable to perfectly foresee the future, it is unlikely that Congress will be more prescient in 2006-07. Indeed, the speed and uncertainty of change in telecom has increased dramatically in recent years compared to the relatively stable and predictable decade that preceded the 1996 law, so today's lawmakers will have an even more difficult time trying to write forward-looking policies and "future-proof" statutes.

This article suggests in Part II an approach to developing a regulatory system that will be compatible with the rapid changes and uncertainty which are likely to characterize telecommunications for the foreseeable future. It starts with the proposition that much of the dissatisfaction with the current system is due to the regulatory gridlock that, among other things, has seriously hampered the recovery of the telecom industry. Gridlock results because it is difficult for the Federal Communications Commission (FCC) to adapt rules, regulations, and

1. This article is based on a report released on October 29, 2004 at CITI's conference on "Remedies for Telecom Recovery: One Year Later." *See* Robert C. Atkinson, Dir. of Policy Res., Columbia Inst. for Tele-Information, Report at Remedies for Telecom Recovery II: What Can the Government Do to Help Recovery? (Oct. 29, 2004), http://www.citi.columbia.edu/research/recovery2/CITI_RegulatoryUpdate04.pdf. That report, in turn, incorporated recommendations made in October 2003 at CITI's initial "Remedies for Telecom Recovery" conference. *See* Robert C. Atkinson, Dir. of Policy Res., Columbia Inst. for Tele-Information, Report at Remedies for Telecom Recovery: Regulation & Government Policy (Oct. 3, 2003), http://www.citi.columbia.edu/CITI_Regulation_advisorycomm.pdf.

policies to address fast-developing and changing issues in a timely fashion. This difficulty is compounded because the 1996 Act creates a logjam that makes it difficult to resolve localized issues locally, so matters that can and should be handled at the state level clog the federal system. In Part III, the article suggests ways to reduce gridlock, including some solutions that would not need new legislation and some that would.

However, the article then suggests in Part IV that the existing regulatory system, even if less gridlocked, will still be too rigid and inflexible to accommodate fast-changing technological and marketplace circumstances. It therefore proposes the legislative solution of replacing the existing static regulatory system with one that can adapt with greater ease to different and ever-changing circumstances. The article concludes in Part V that a "future-proof" regulatory system can be achieved by a simple, flexible new statute that relies on market forces wherever possible and, for matters where the regulation is necessary, simple regulatory principles and procedures rather than gridlock-inducing statutory micromanagement of the sort included in the 1996 Act. The article suggests many of the principles and procedures that should be included in such a law.

## I. AVOIDING GRIDLOCK: A FUNDAMENTAL PROBLEM FOR THE TELECOM INDUSTRY IS A GRIDLOCKED REGULATORY PROCESS

A great challenge facing policymakers and telecom industry managers and investors is whether critical government policies and regulations can be changed rapidly enough to stay in step with the rapid, unpredictable changes of a volatile and fundamentally unstable telecom industry.[2] If management and investors don't know what the basic government rules are, there will be a natural tendency–exacerbated by the historic 2000-01 financial crash of telecom investments–to hesitate and to wait until the rules get clearer.[3] Such hesitation is bad for the

2. From the time of the consolidations that created the telephone monopolies that gave rise to the Communications Act of 1934 until quite recently, the telephone business was very stable and predictable. CITI's "Remedies for Telecom Recovery" project, *supra* note 1, recognized that the recent "boom and bust" might be the beginning of a long period of fundamental instability in telecommunications and that regulators, managers and investors have little or no experience in dealing with such a radically different environment. The CITI project reports are available at http://www.citi.columbia.edu/hold.html. For other materials based on the project *see* Eli Noam, *How to Cope with the New Volatility*, AMERICA'S NETWORK, Oct 1, 2003, http://www.americasnetwork.com/americasnetwork/article/articleDetail.jsp?id=71237; Eli Noam, *The Effect of Deregulation on Market Concentration,* 4 COLUM. SCI. & TECH. L. REV. 8 (2003); Eli Noam, *How Telecom Is Becoming a Cyclical Industry, and What to Do About It* (June 28, 2002) (unpublished manuscript, available at, http://www.citi.columbia.edu/elinoam/articles/cyclicality.htm).

3. Therefore, once an important issue is "teed up" on the regulatory or government policy agenda, the substance of the subsequent decision may be less important to the health of

economy, innovation, competitiveness, and consumer welfare.

Two broad categories of regulatory decisions that are of great interest to telecom managers and investors are revenue regulation and competition policy. The level of interest is high because these are the sorts of regulations which most directly affect business rewards and risks (e.g., profits). Since the passage of the Telecom Act, revenue regulation and competition policy have been intertwined at the Federal level in five areas: access charges,[4] reciprocal compensation,[5] Universal Service,[6] Bell

---

the telecom sector than the speed at which a reasonably final decision can be reached.

4. Access charges are fees paid by long distance telephone companies to local telephone companies to originate or terminate a long distance call. They were created as the result of the 1984 break-up of the Bell system to maintain the flow of subsidies from long distance to local services and from urban areas to rural areas in order to keep the prices of local services lower than they otherwise would be, particularly in the rural areas. Since the Bell System break-up, the FCC has issued a series of "access charge" Orders, the trend of which has been to lower the charges and move responsibility for paying the charges from carriers to customers to encourage a more economically rational system. *See, e.g.*, Access Charge Reform, Price Cap Performance Review for Local Exchange Carriers, Transport Rate Structure & Pricing End User Common Line Charges, *First Report & Order*, 12 FCC Rcd. 15,982 (1997); Access Charge Reform, *Fifth Report & Order*, 14 FCC Rcd. 14,221 (1999); Access Charge Reform, Price Cap Performance Review for Local Exchange Carriers, Low-Volume Long-Distance Users, & Federal-State Joint Board on Universal Service, *Sixth Report & Order*, 15 FCC Rcd. 12,962 (2000); Access Charge Reform, Reform of Access Charges Imposed by Competitive Local Exchange Carriers, *Eighth Report and Order and Fifth Order on Reconsideration*, 19 FCC Rcd. 9108 (2004). However, changes in access charges have complex interactions with Universal Service and competition policy so the "access charge" Orders tend to be tentative, muddy compromises. *See, e.g.*, Access Charge Reform, Price Cap Performance Review for Local Exchange Carriers, Low-Volume Long Distance Users, Federal-State Joint Board On Universal Service, *Sixth Report & Order*, 15 FCC Rcd. 12,962, 12,971-72, 12,974-77 (2000).

5. "Reciprocal compensation" is the fee paid by one local carrier to another local carrier when one carrier originates a call and the other terminates it. Prior to the advent of local telephone competition in the early 1990s, local traffic was exchanged between adjacent local telephone service monopolies under a long established system known as "separations and settlements" that often involved little or no exchange of cash. When new local competitors sought to exchange traffic with the incumbent local telephone companies using the "separations and settlements" system, the incumbents refused and instead proposed to exchange traffic on the basis of the "access charges" used for long distance calls, *supra* note 4. Because "access charges" included various subsidies, they were higher than the retail prices of the local telephone service, making it difficult or impossible for a new entrant to offer a profitable competing local service if access charges were applied. The disputes between local incumbents and new entrants were resolved with varying degrees of success by State regulators. The Telecommunications Act attempted to make the better State solutions national policy by requiring local traffic to be exchanged at rates that reflect only "a reasonable approximation of the additional costs" of terminating the call. 47 U.S.C. § 252(d) (2)(A)(ii) (1996). Even with this clear pricing standard, "reciprocal compensation" has remained as a point of major dispute since 1996.

6. "Universal Service" is a policy to ensure that every citizen has access to reasonably priced basic telephone service, regardless of the actual cost of providing the service or the citizen's ability to pay. Central to this policy is the subsidization of high cost areas and low income consumers and, more recently, assistance to schools, libraries and rural health care facilities. When telephone service was a monopoly, the support of universal service was embedded in a complex system of subsidies approved by State and federal regulators. Business

company entry into long distance,[7] and unbundled network elements[8] (particularly the UNE-Platform[9]). And in the ten years since 1996, the first three of these areas remain unresolved, the fourth (Bell long distance entry) was completed in late 2003 and the fifth (UNEs) was largely (but not completely) resolved only in 2004. The inability of the existing regulatory system to achieve final, clear decisions on these (and other) critical decisions within a short period of time can best be described as

---

services and services for consumers in urban areas were priced above costs to generate a surplus that would subsidize retail rates in high cost rural areas and for low income individuals. Long distance services were priced higher than costs to provide a subsidy to local rates. New competitors naturally focused their efforts on offering business services in low cost urban areas, the very services and geographic markets generating the subsidies to residential consumers and rural areas. This presented regulators with a dilemma: authorizing and encouraging competition might have an adverse impact on politically-sensitive local telephone rates. Incumbent telephone companies used the prospect of huge local telephone rate increases to encourage regulators to slow or even halt the development of competition. The never-ending disputes over the level of access charges and reciprocal compensation were largely about the preservation of the subsidy flows.

§ 254 of the Telecommunications Act of 1996 sought to maintain universal service subsidies without impeding the development of competition by substituting explicit subsidies for the implicit subsidy system used in the monopoly era. The goals of Universal Service, as mandated by the Telecommunications Act of 1996, are: to promote the availability of quality services at just, reasonable, and affordable rates; to increase access to advanced telecommunications services throughout the Nation; and to advance the availability of such services to all consumers, including those in low income, rural, insular, and high cost areas at rates that are reasonably comparable to those charged in urban areas *See* 47 U.S.C. § 254 (2006). Despite the Telecom Act's admonition that all subsidies must be explicit, implicit subsidies remain in 2006.

7. The 1982 Modifications of Final Judgment MFJ was an antitrust consent decree that broke up the Bell System into seven Regional Bell Operating Companies (RBOCs) and AT&T, which provided long distance service and manufactured telecommunications equipment. United States v. AT&T Corp., 552 F. Supp. 131 (D.D.C. 1982). The MFJ prohibited a Bell Operating Company (BOC) from providing long distance service until local competition developed sufficiently to neutralize the BOCs' local market power. No BOC qualified to offer long distance service under the MFJ. § 271 of the 1996 Act superseded the MFJ and established a "14 point checklist" and some other criteria which RBOCs would have to satisfy in order to qualify to provide long distance service. 47 U.S.C. § 271(c)(2)(B) (1996).

8. Unbundled Network Elements or "UNEs" are piece-parts of one carrier's telecom network that are provided to other carriers so that the second carrier can augment its own network. The Telecommunications Act includes provisions concerning the duty of incumbent local telephone companies to make UNEs available and when that duty attaches. 47 U.S.C. §§ 251(c)(3), 251(d)(2) (2005).

9. The Unbundled Network Element Platform or "UNE-P" consists of all the network elements needed to provide basic telephone service. The FCC's approval of the UNE-P was extremely controversial. Incumbents argued that the UNE-P could not have been intended by Congress because it made the Act's resale provisions, § 251(c)(4), irrelevant since the UNE-P provided the same functionality at considerably lower cost. They also argued that the UNE-P did not satisfy the "necessary and impair" standard established by § 251(d)(2) that determines when unbundled elements must be offered. New entrants, on the other hand, argued that the UNE-P was an essential first step in the development of competitive residential telephone service. *See generally* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS 99-108 (2005).

regulatory gridlock.

### *A. General Reasons for Regulatory Gridlock*

There are at least three general reasons for regulatory gridlock in telecommunications. First, the telecom industry itself is composed of fractious and competing segments that are so inordinately suspicious of each other that any change thought to benefit one segment will be opposed ferociously by that segment's competitors. Since it is much easier to block a change than to make a change in a legislative or regulatory proceeding, the industry itself often gridlocks the regulatory and public policy process.

Second, many policy changes that might benefit the overall telecom industry are likely to be at the expense of consumers. This is particularly true with respect to changes that reduce competition or increase retail prices. Consumers have benefited greatly from competition and innovation during recent years and it will be difficult to convince regulators or legislators that there is a need to make changes that disadvantage consumers simply to help multi-billion dollar enterprises.

Finally, even without industry and consumer interests blocking changes, the due process that the Constitution imposes on changing fundamental law or regulations (including seemingly inevitable appellate litigation) is a slow, ponderous, and uncertain process.[10]

### *B. Telecom Act As a Specific Cause of Gridlock*

The 1996 amendment of the Communications Act seems to be a particular cause of the current gridlock. For all its well-meaning intentions about loosening the grip of government, the Telecommunications Act of 1996 ended up centralizing all fundamental telecommunications policy in the FCC, effectively federalizing the 50 states with respect to local competition[11] and preempting the judicially-supervised modification of final judgment (MFJ) with respect to Bell entry into long distance.[12] Among other objectives, this centralization was intended to satisfy investors' supposed desire for greater certainty

10. *See, generally,* U.S. CONST. amend. XIV ("No State shall. . .deprive any person of life, liberty, or property, without due process of law. . ."); *see also* Richard A. Posner, *Antitrust in the New Economy*, 68 ANTITRUST L.J. 925, 939 (2001) ("The law is committed to principles of due process that limit the scope for summary proceedings, and the fact that litigation is conducted by lawyers before tribunals that are not technically trained or experienced inevitably slows the process.").

11. *See, e.g.*, Roy E. Hoffinger, *Cooperative Federalism Gone Wrong: The Implementation of the Telecommunications Act of 1996*, 2 J. TELECOMM. & HIGH TECH. L. 375 (2003); Gary J. Guzzi, *Breaking Up the Local Telephone Monopolies: The Local Competition Provisions of the Telecommunications Act of 1996*, 39 B.C. L. REV. 151 (1997).

12. 47 U.S.C. § 271 (2005).

and predictability.[13]

However, the Telecom Act did not simply establish broad policy goals – such as competition in all markets and less regulation – and then leave it to the FCC to achieve them. Rather, the statute itself sought to micromanage the implementation of specific regulatory policies. For example, the Act dictated the FCC's work schedule by imposing numerous decisional deadlines;[14] specified three pricing methodologies for carrier interconnections;[15] established nebulous concepts such as "necessary" and "impair" as decisional standards for determining when dominant local carriers are required to offer unbundled network elements;[16] constructed a detailed system for negotiating, mediating, and arbitrating interconnection agreements (with substantial regulatory involvement in the arbitration process);[17] and specified a 14-point checklist to be satisfied before a Bell company could offer long distance services.[18]

This statutory micromanagement, in turn, has led to gridlock as evidenced by the seven years (1996-2003) it took for Bell company entry into long distance services,[19] eight years (and counting) to unbundle network elements to facilitate local entry,[20] and the continued existence

13. *See* Hoffinger, *supra* note 11 at 377, 387 n.53.

14. *See, e.g.*, 47 U.S.C. § 251(d)(1) (2005) (requiring FCC to complete implementation of § 251 within 6 months), 47 U.S.C. § 254(g) (2005) (requiring FCC to adopt rules requiring rates for long distance service in rural and high cost area be no higher than rates charged in urban area within 6 months). Shortly after it was enacted the FCC prepared a voluminous "Implementation Schedule for the Telecommunications Act of 1996" which noted all the statutory tasks and timelines. *See* FEDERAL COMMUNICATIONS COMMISSION, DRAFT IMPLEMENTATION SCHEDULE FOR THE TELECOMMUNICATIONS ACT OF 1996 (1997), http://www.fcc.gov/Reports/implsched.html.

15. 47 U.S.C. § 252(d)(1)-(3) (2005).

16. 47 U.S.C. § 251(d)(2) (2005).

17. 47 U.S.C. § 252 (2005).

18. 47 U.S.C. § 271(c)(2)(B) (2005).

19. The first § 271 application was filed in January 1997 but was withdrawn. The next five applications were denied. The first successful application was approved in December 1999 with the final application granted in December 2003. *See* FEDERAL COMMUNICATIONS COMMISSION, RBOC APPLICATIONS TO PROVIDE IN-REGION, INTERLATA SERVICES UNDER § 271 (2005), http://www.fcc.gov/Bureaus/Common_Carrier/in-region_applications/.

20. *See generally*, NUECHTERLEIN & WEISER, *supra* note 9, at 80-82, 99-108. The history of this period of repeated FCC attempts to regulate "UNE" unbundling (and the subsequent judicial invalidation of each) is a complex and tortured one. Beginning with its August 1996 *Local Competition Order*, the FCC attempted to comply with the 1996 Telecom Act's impairment standard as mandated by § 252(d)(1), which limited the number of network elements subject to unbundling under § 251(c)(3). *See* Implementation of the Local Competition Provisions of the Telecommunications Act of 1996, *First Report & Order*, 11 FCC Rcd 15,499 (1996) [hereinafter "*Local Competition Order*"]. In 1998, the Supreme Court rejected this *Order*, remanding the matter back to the FCC. *See* FCC v. Iowa Utilities Board, 525 U.S. 366 (1999). The FCC addressed the matter again in Nov. 1999, issuing its *UNE Remand Order* and increasing the scope of unbundling to include previously ignored elements such as dark fiber. *See* Implementation of the Local Competition Provisions of the

of implicit subsidies in telecom rates despite the Telecom Act's directive to eliminate them.[21]

Recently, the nature of the long standing intra-industry conflicts that caused so much gridlock may have changed as AT&T and MCI, the two largest long distance carriers, have been absorbed into SBC (renamed AT&T) and Verizon, respectively, and as competitive local exchange carriers (CLECs) virtually disappear. As a result, the surviving Bell-based telephone companies won't have to contend with (be gridlocked by) traditional industry rivals. However, as the telephone industry evolves into broadband communications services, it is bumping into new and powerful rivals that will have the capability to continue the gridlock for the foreseeable future. On one hand, the cable television industry is rapidly becoming a new counterweight to the ILECs as cable companies become serious rivals in the telephone business and as the major telecom companies begin to enter the television business. On the other hand, both the telephone and cable industries are beginning to clash with powerful adjacent information industries—such as Internet

Telecommunications Act of 1996, *Third Report & Order*, 15 FCC Rcd. 3,696 (1999) [hereinafter "*UNE Remand Order*"]. This effort was also rejected by the courts in the 2002 *USTA I* decision, in which the D.C. Circuit chided the FCC for failing to meet the § 251(d)(2) unbundling standards. *See* U.S. Telecom Ass'n v. FCC, 290 F.3d 415, 429 (D.C. Cir. 2002) [hereinafter "*USTA I*"] ("[U]nbundling is not an unqualified good. . .(it) comes at a cost. . ."). The Commission tried once more to address "UNE" unbundling rules pursuant to § 251(d)(1), issuing its monstrous *Triennial Review Order* in 2003, but in 2004 was once again rejected by the D.C. Circuit in *USTA II.* S*ee* Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, *Report & Order & Order on Remand & Further Notice of Proposed Rulemaking*, 18 FCC Rcd. 16,978 (2003) [hereinafter "*Triennial Review Order*"]; U.S. Telecom Ass'n v. FCC, 359 F.3d 554, 360 U.S. App. D.C. 202 (D.C. Cir. 2004) [hereinafter "*USTA II*"]. At the time, the industry gave little regard to *USTA II*, anticipating a successful appeal to the Supreme Court, which appeared to be leaning in a favorably pro-competition direction. NUECHTERLEIN & WEISER, *supra* note 9, at 104. Against industry expectations, however, Solicitor General Olson decided in June 2004 not to appeal *USTA II.* The FCC's most recent attempt at "UNE" regulation came in its December 2004 *Order on Remand*, responding to *USTA II* with interim rules (which, not surprisingly, were subsequently challenged in the D.C. Circuit.) *See* Unbundled Access to Network Elements, *Order & Notice of Proposed Rulemaking*, WC Dkt. No. 04-313 et al., 2004 WL 1900394 (Aug. 20, 2004). The net effect of this swinging pendulum, from attempted regulation to judicial invalidation and back again, was clear: the "UNE" regulatory waters were sufficiently muddied to the point of detrimentally affecting business strategies. Lacking clear, consistent, reliable guidance from either the FCC or the courts, companies became understandably hesitant to dive into these dark, turbulent waters, and telecom investors (and the tech industry in general) suffered. In July 2004, for example, following the publication of *USTA II*, AT&T announced it would no longer seek new customers for conventional telephony services. NUECHTERLEIN & WEISER, *supra* note 9, at 108; FCC v. Iowa Utilities Board, 525 U.S. 366 (1999).

21. 47 U.S.C. § 254(k) (2005) (prohibiting cross-subsidization by carriers); 47 U.S.C. § 254(b)(5) (2005) (requiring universal service support mechanisms to be "specific, predictable and sufficient. . .").

content providers like Google and Microsoft[22]—which will inevitably further gridlock resolution of controversies submitted to regulators. Thus, despite the consolidation of the traditional telecom industry, the potential for gridlock is still great.

## II. REDUCING REGULATORY GRIDLOCK WILL ENCOURAGE TELECOM RECOVERY

If the gridlock of the existing regulatory system is a substantial obstacle to recovery and expansion of the telecom and information sector, what are the remedies for regulatory gridlock? There are two obvious solutions: first, reduce opportunities for gridlock by reducing the scale and scope of regulation wherever possible, and second, streamline regulatory processes and procedures wherever and whenever regulation is required so that final decisions can be reached quickly.

Some of the anti-gridlock solutions described below may require changes in the federal and State statutes.[23] However, many process and procedural changes can be implemented by regulatory agencies without legislation, so some rapid self-reform is feasible.

### *A. Reduce Gridlock By Adopting And Then Following Guiding Principles And Policies*

One way to reduce gridlock is to minimize the tendency for regulators to spread their resources too thinly by allowing themselves and their staffs to become entangled in non-essential matters. In the absence of legislative micromanagement that requires regulators to perform specific duties within certain timeframes,[24] regulators can reduce gridlock by only initiating proceedings which are consistent with a small but clearly described set of fundamental guiding principles — the regulatory agency's "strategic plan." Articulating and then adhering to a clear strategic plan will make regulatory decision-making quicker, more consistent, and more predictable, which, in turn, will engender investor confidence and minimize the likelihood or success of appellate litigation.

Each regulatory agency will have to develop and publish its own

22. *See, e.g.*, John Markoff, *Coming Soon to TV Land: The Internet, Actually*, N.Y. TIMES, Jan. 7, 2006, *available at* http://www.nytimes.com/2006/01/07/technology/07video.html?ei=5090&en=afe0c357a1b1d976&ex=1294290000&partner=rssuserland&emc=rss&pagewanted=print; W. David Gardner & Laurie Sullivan, *Google, Microsoft At It Again—This Time It's VoIP*, INFORMATIONWEEK, Sept. 5, 2005, *at* http://www.informationweek.com/story/showArticle.jhtml?articleID=170700308&tid=5979.

23. Statutory changes that would reduce regulatory gridlock are included in Section V, *infra*, which suggests what should be included in a new telecom law.

24. This is one way that the Telecommunications Act of 1996 created gridlock. *See supra*, note 19.

strategic plan within the requirements of its governing law. Developing such a plan would also identify areas where the governing law would need to be changed to accommodate it. Fundamental guiding principles might include the following examples:[25]

Competition is to be the preferred regulatory mechanism in every market to encourage fair prices, innovation, and efficiency.

In markets where competition is demonstrably insufficient to achieve these goals, regulation should be applied to the minimum extent required to protect consumers from pricing and service abuses.

The allocation of regulatory authority and responsibility between States and the Federal government should be based not on the increasingly unknowable jurisdiction of the traffic but on the basis of which agency is best positioned and best equipped to handle each specific regulatory responsibility.

Policies based on the outdated and now erroneous assumption that the traditional voice telephone business is stable and a foundation for all other services will not be sustainable. The emergence of wireless and Internet telephone services is but the latest example of the fallacy.

No industry structure can be assumed to be stable, permanent or universal: sustainable policies must be able to accommodate different industry structures in different geographic areas, ranging from multiple competitive infrastructures to duopoly and even monopoly.

Since competing infrastructures may not be economically sustainable (particularly in smaller markets) if infrastructure operators are limited to providing only commodity transport services, infrastructure operators should be able to offer value-added content. However, regulation of the infrastructure would be appropriate if the infrastructure operator has unfairly restricted consumers' ability to access content provided by others, including discriminating between content providers.[26]

"Essential facilities" might need to be regulated if consumer abuse occurs in the absence of regulation. For example, the ILECs' ubiquitous copper loop systems cannot be duplicated as a practical matter, and yet they are essential for competing circuit-switched voice-grade services. The copper loop will become less essential and then non-essential as

25. Many of these possible principles are included in the Progress and Freedom Foundation's "Digital Age Communications Act" (DACA) proposal and the "Digital Age Communications Act of 2005" introduced in the Senate on Dec. 15, 2005 by Sen. James DeMint. *See* PROGRESS & FREEDOM FOUNDATION, THE DIGITAL AGE COMMUNICATIONS ACT PROJECT, http://www.pff.org/issues-pubs/books/051207 daca-usf-2.0.pdf; Digital Age Communications Act of 2005, § 2113, 109th Cong. (2005), *available at* http://www.pff.org/issues-pubs/other/other/051215dacabill.pdf. Although the author of this article participated in some aspects of the PFF project, the guiding principles included in the article were first published in the report referenced in Note 1 and therefore predated the DACA work.

26. This is sometimes called "net neutrality" or "open access."

wireless and Internet telephone services become widespread alternatives to traditional telephone service. But new facilities may become essential to future services and might need to be regulated if an operator's control of the essential facility results in consumer abuse.

Universal Service is an important national goal but, because Universal Service subsidies have little to do with telecommunications service and much to do with social issues, they should be managed not by telecom regulators but by government agencies experienced with administering social programs.

### *B. Reduce Gridlock By Deregulating Retail Services*

Historically, one obvious gridlock-causing sticking point has been the regulation of retail rates and service quality. State public utility commissions regulated basic local telephone services for two reasons: 1) to prevent abusive pricing of essential services by monopoly or dominant suppliers; and 2) to make basic service more affordable in high cost areas and to residential consumers through an elaborate system of cross-subsidies.[27]

Both rationales are artifacts of the monopoly era; they are much harder to justify in an environment which is more competitive, at least for the immediate future. The elaborate rate proceedings themselves can cause uncertainty for considerable periods of time and are massive drains on regulatory resources. But just as importantly, the social subsidy ripple effects of rate regulation, such as Universal Service and access charges,[28] create their own gridlock and uncertainty.

If a market is reasonably competitive, there would be little consumer protection justification for retail service regulation. This principle worked well in the long distance market: once there was enough competition from MCI, Sprint, and others so that AT&T was determined to be "non-dominant," the FCC eliminated retail price regulation of long distance services.[29] Similarly, prices of wireless telephone services have

---

27. *See* Philip J. Weiser, *The Ghost of Telecommunications Past*, 103 MICH. L.R. 1671, 1677-78 (2005); *see generally* M. L. MUELLER, JR., UNIVERSAL SERVICE: COMPETITION, INTERCONNECTION, AND MONOPOLY IN THE MAKING OF THE AMERICAN TELEPHONE SYSTEM (1997).

28. As explained in notes 4, 6 and 27, *supra*, the access charge and universal service issues have been an unending source of dispute and litigation since 1996 and even before. That is because access charges–fees charged by local carriers to originate and terminate long distance calls–have been the source of much of the implicit subsidies that support universal service. Thus, a proposed reduction in access charges raises the specter of reduced subsidies and concomitant increases in politically-sensitive local telephone rates, leading to litigation and temporary compromises but not to final resolution.

29. Motion of AT&T Corp. to Be Reclassified as Non-Dominant Carrier, *Order*, 11 F.C.C. Rcd. 3,271 (released Oct. 23, 1995). "Dominant" carriers were subject to regulation because they have "market power" (the ability to control process)). *See*, Policy and Rules

not been regulated since no cellular carrier has (so far) been able to dominate that market.

If there is sufficient actual and potential competition in a geographic market for every retail telecommunications service, including basic local telephone service, regulation should be unnecessary for consumer protection. The reality is that basic telephone service consumers in most (but certainly not all) geographic markets currently have alternatives to the ILEC through wireline resellers, numerous wireless services providers, and, increasingly, from VoIP[30] provided over telco and cable broadband services.[31] While competitive alternatives from CLECs using the UNE-Platform will disappear as the result of FCC action,[32] consumers' opportunity for having VoIP service from cable TV companies, as well as from independent service providers such as Vonage, is increasing rapidly. Therefore, in most significant markets it is difficult to imagine that ILECs could abuse their customers by raising prices or offering poorer quality service without suffering substantial competitive losses.

Of course, there will be a few geographic markets where there is insufficient competition to protect consumers from abuse.[33] However, market-by-market deregulation proceedings should be avoided. Hundreds (or even thousands) of deregulation proceedings would all but guarantee gridlock and the entire regulatory system would grind to a halt. Rather, it would be better to "flash cut" retail rate deregulation in all markets and then observe whether and where any abuse of consumers actually occurs. There are plenty of competitors and consumer advocates to bring any suspected abuse to state and federal regulators' attention. Where consumer abuse is demonstrated, swift (and even harsh)[34] re-regulation would be appropriate and necessary.

---

Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefore, *First Report & Order*, 85 F.C.C.2d 1, 20 (1980).

30. Voice over Internet Protocol.

31. According to the FCC's Local Competition Report for calendar year 2004 (the most recent available): "At the end of 2004, end-user customers obtained local telephone service by utilizing approximately 145.1 million incumbent local exchange carrier (ILEC) switched access lines, 32.9 million competitive local exchange carrier (CLEC) switched access lines, and 181.1 million mobile wireless telephone service subscriptions." Press Release, Fed. Commc'ns Comm'n, Federal Communications Commission Releases Data on Local Telephone Competition (July 8, 2005) http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/lcom0705.pdf.

32. Unbundled Access to Network Elements, *Order on Remand*, 20 F.C.C. Rcd. 2533 (2004); *see also* Press Release, Fed. Commc'ns Comm'n, FCC Adopts New Rules for Network Unbundling Obligations of Incumbent Local Phone Carriers (December 15, 2004), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-255344A1.pdf.

33. *See, e.g.*, Mountainsage.org, *infra* note 51.

34. If the reaction to the first few instances of consumer abuse were harsh, abusive behavior by other service providers would be deterred.

Since local, intrastate telephone service is currently regulated by each State, Federal preemption of State regulation, presumably through Federal legislation, would be required to assure retail rate deregulation on a national basis. Such legislation should empower the FCC, in consultation with the States, to determine a "flash cut" date (perhaps within one year of enactment) and establish the criteria that would justify re-regulation in particular markets.[35] State Commissions would then be responsible for applying the FCC's re-regulation criteria and the FCC would hear any appeals of a State's decision to re-regulate.

In the absence of Federal legislation, or perhaps as experiments to justify a national policy (see discussion below regarding the value of experimentation), some States could implement retail rate deregulation by decision of the State's regulatory commission under existing State law. In other States, legislation would be required to de-regulate or give State Commissions the authority to deregulate.

Since retail rate regulation is one means for artificially keeping basic service rates below cost in some markets and for favored classes of consumers, abolition of retail rate regulation would mean that Universal Service objectives would have to be achieved by means other than implicit cross-subsidies within a carrier's rate structure. This would be consistent with the thus-far-ignored Congressional mandate of eliminating such implicit subsidies.[36]

If complete retail rate deregulation is too radical and consideration of such an action would itself cause more gridlock, the regulation of cable television rates might provide a more conservative model. Cable rate regulation has been eliminated, except for "basic" cable, with remaining regulation focused on regulating "access" to the cable television system. Analogously, only the most basic "lifeline" telephone service would be rate-regulated.

### *C. Reduce Gridlock By Resolving All Carrier-to-Carrier Issues Only Through Interconnection Agreements and Commercial Arbitration, Never By Regulators*

Another major source of regulatory gridlock is related to the resolution of carrier-to-carrier business issues, including: reciprocal compensation, access charges, UNEs and UNE pricing, and performance standards. Not only do these matters consume much of the resources at regulatory agencies, they pit industry sectors and companies against each

35. Consumer abuse should be the touchstone of regulation and re-regulation. Abuse of competitors can and should generally be addressed in antitrust and commercial law. Generally, regulators should not become entangled in disputes between competitors over commercial arrangements if such involvement is not needed to avoid a secondary abuse of consumers.

36. *See* 47 U.S.C. § 254(k) (2005).

other, with the usual result that each side neutralizes the other so much that little progress (but more gridlock) is made despite prodigious exertion.

Resources could be saved and the issues removed almost entirely from the regulatory process (and therefore gridlock) if service providers had to resolve ***all*** of these complex business issues in the same manner as "normal" businesses: through bilaterally negotiated contracts and agreements. Then, at most, communications regulators would only have to be involved in matters which the parties have been unable to resolve.

Under Sec. 252 of the Communications Act,[37] if carriers can't negotiate interconnection agreements, they are entitled to have state regulators arbitrate the dispute. The Act doesn't specify how the arbitrations should be conducted, presumably leaving it up to each state to develop an arbitration procedure. Unfortunately, many states treated the arbitrations as normal regulatory proceedings despite the Congressional intent to establish a deregulatory means for resolving carrier-to-carrier interconnection disputes.[38] As a result, the arbitrations often become just another regulatory proceeding and are likely to be gridlocked like one.

To avoid becoming entangled in commercial issues (for which they have no particular experience or expertise) and to avoid the gridlock that normally occurs in a contested regulatory proceeding, state regulators should appoint experienced commercial arbitrators (paid for by the parties) to conduct the arbitration. This is appropriate: where the disputes are with respect to commercial arrangements, not regulatory principles, it would be best to let people experienced in resolving business matters make the commercial decision.

Additionally, unless the parties to the arbitration agree on some other procedure (and to avoid gridlock), the default arbitration process should be "baseball arbitration," where the arbitrator can only choose between the parties' final package of offers: one side will win *all* the disputed issues and the other side will lose on *every* issue. The prospect of baseball arbitration should raise the risk to both parties and encourage both parties to be more reasonable (approach the middle) in their final offers since the arbitrator will generally choose the most reasonable final offer.[39] Ideally, baseball arbitration would result in a settlement between

37. 47 U.S.C. § 252 (2005).

38. *See*, H.R. Rep. No. 104-204, at 48 (1995), *reprinted in* 1996 U.S.C.C.A.N, Legislative History 10, 11; H.R. Rep. No. 104-458, at 113 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. Legislative History 124.

39. *See* Charles E. Rumbaugh, *Having Trouble Getting to the Negotiation Table? Try Baseball Arbitration*, 49, 2002 CONTRACT MGMT. 48, (Oct. and Nov. 2002), available at http://www.rumbaugh.net/docs/ADR_BB_Part1.pdf and http://www.rumbaugh.net/docs/ADR_BB_Part2.pdf.

the parties, as it usually does in baseball.

This proposal does *not* mean that regulators and regulatory policy wouldn't be involved in establishing a framework for arrangements between carriers. Regulators would have three roles: establishing arbitration principles; reviewing arbitrators' decisions for conformance with those principles; and adopting conforming arbitration decisions as agency decisions.

Instead of becoming entangled in the micromanagement of countless specific business disputes, regulatory policies and objectives would be incorporated into the arbitration standards to be utilized by the commercial arbitrators. Indeed, by knowing the regulator-approved arbitration standards, parties would be better able to assess what the arbitrator's decision is likely to be, making it more likely that there would be more settlements and fewer unresolved issues to arbitrate (i.e., less gridlock) in the first place.

To avoid gridlocking the process of determining arbitration standards, regulators should set a few simple policy goals rather than engaging in predictive micromanaging. These principles might include maximizing network interconnectivity, economic efficiency, retail competition, consumer benefits, and network reliability. Regardless, the essential charge to the arbitrator should be to pick the most commercially reasonable and sensible result.

If the State Commission rejects the arbitrator's decision as being incompatible with the arbitration standards or the law, it should *not* try to insert its judgment and rewrite the decision. That would be a gridlock-inducing step. Rather, the State Commission should send the issue back to another arbitrator with an explanation of why it rejected the earlier decision.

Another way to minimize gridlock involving interconnection agreements is to allow carriers to adopt (or "opt in") to other carriers' existing agreements rather than negotiating and arbitrating their own. Sec. 252(i)[40] requires ILECs to provide interconnection and unbundled network elements included in an Interconnection Agreement to other competing carriers. This is an excellent provision in theory: it prevents collusive or unreasonably discriminatory deals and saves smaller carriers from the expense of negotiating and arbitrating their own deals if another carrier's arrangements are satisfactory. But even this provision was embroiled in its own longstanding controversy. The FCC initially permitted other parties to "pick and choose."[41] In response, incumbents

40. 47 U.S.C. § 252(i) (2005).

41. "Pick and choose" means that a CLEC can assemble its own Interconnection Agreement with an ILEC by "picking" provisions from various Interconnection Agreements previously entered into by the ILEC. The FCC's interpretation of the statute was approved by

refused to make individual bilateral arrangements for fear of being picked to death. More recently, the FCC reversed itself and determined that Sec. 252(i) doesn't require "pick and choose" and that an "all-or-nothing" rule will promote real negotiation.[42]

By fixing the interconnection agreement process, there would be no need for endless speculation about whether UNE-P is good, bad, or indifferent or whether "bill & keep" is a better access charge and reciprocal compensation system. The real-world results of a variety of interconnection agreements – the results of private, commercial experiments – would speak for themselves. The real-world experience can then be applied to subsequent negotiations, arbitrations, and the few regulatory decisions that still might be needed.

Even though regulators would be, at most, minimally involved in carrier-to-carrier issues, it is important to note that anticompetitive behavior by one carrier (such as leveraging bottleneck facilities) would be subject to private antitrust action and civil antitrust enforcement by the US Department of Justice and State Attorneys General.

### *D. Reduce Gridlock By Developing Better Evidence Through Experiments*

Better evidence results in better decisions. This truism applies as well to telecom regulatory decisions as any other. So, what is the best evidence for telecom regulatory decision-making?

Much of the regulatory gridlock can be attributed to the dueling theories, studies, and expert opinions submitted by opposing parties in attempts to "prove" the future. This leaves regulators—particularly the FCC—to choose from this predictive evidence whatever supports the policy outcome they prefer. This is risky decision-making and subject to seemingly endless appeals because it looks (and inevitably is) arbitrary and capricious.

Experimental evidence (as distinguished from predictive evidence) is more reliable and of much higher quality, making regulatory decisions based on such evidence both less risky and more sustainable.

To illustrate the value of experimentation to investors and regulators, consider local telecom competition. With respect to local

---

the Supreme Court. *See* Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, *First Report & Order*, 11 F.C.C. Rcd. 15,499, 16,137 (1996); AT&T Corp. v. Iowa Utils. Bd., 525 U.S. 366, 395-96 (1999).

42. "Opt in" or "all-or-nothing" means that a CLEC would be able to select one of the ILEC's other Interconnection Agreements in its entirety (rather than "picking and choosing" provisions from all prior agreements) as its Interconnection Agreement with that ILEC. *See generally* Review of the Section 251 Unbundling Obligations of Incumbent Local Exchange Carriers, *Second Report & Order*, 19 FCC Rcd. 13,494 (2004).

competition, it is important to recognize that the Telecom Act of 1996 was neither revolutionary nor innovative. Rather, the Act largely codified into national law and policy the results of many local competition experiments that had been conducted by State public utility commissions between 1985 and 1995.[43]

Many observers claim that this state-by-state experimentation — with its admittedly untidy look of "muddling through"— did not provide the certainty and predictability sought by investors. Ironically, and not appreciated by investors at the time and perhaps even today, "muddling through" was and is much less risky than a single federal policy, particularly when the federal system gets gridlocked in interminable due process. That is because "muddling through" in the States allowed for a continuous and low-risk iterative process of field experimentation, testing, and fine tuning of business strategies and public policies before irrevocable, major investment bets were placed on a national scale.

Historically, when State experiments were deemed to be successful, other States and then the FCC made similar decisions.[44] But when State experiments were judged to have failed, they were rarely repeated by other States and, fortunately, did not become national policy under the FCC.

The advent of the Telecom Act virtually halted State experiments as the States waited, and waited, and waited for some final guidance from the FCC and the Courts about the new law. At the same time, the Act did not empower or encourage the FCC to undertake its own experiments. As a result, after 1996 every major regulatory issue became a single high-risk roll of the federal dice. Every FCC decision – because it had national application – literally became a multi-year federal case and led not to finality but to litigation, with fundamental decisions often being made not by an expert agency but by judges and their law clerks.

---

43. For example, the FCC outlined New York State's leading role in the development of local competition prior to the 1996 Telecom Act in its New York § 271 decision. Application by Bell Atlantic New York for Authorization Under Section 271 of the Communications Act to Provide In-Region, InterLATA Service in the State of New York, *Memorandum Opinion & Order*, 15 FCC Rcd. 3,953, 3,989-4,077 (1999).

44. Consider, for example, the FCC's landmark "collocation" decision through which the FCC first encouraged local telecom competition by requiring ILECs to allow CLECs to interconnect to the ILECs' local networks inside the ILEC's central offices. The FCC's Order cited the success of a number of earlier interconnection decisions by State public utility commissions. *See* Expanded Interconnection with Local Telephone Company Facilities, *First Report & Order*, 7 FCC Rcd. 7,369 (1992); *First Reconsideration*, 8 FCC Rcd. 127 (1993), *Second Reconsideration*, 8 FCC Rcd. 7,341 (1993), *Second Report & Order*, 8 FCC Rcd. 7,374 (1993); vacated in part and remanded, *See also* Bell Atlantic Telephone Co. v. FCC, 24 F.3d 1,441 (D.C. Cir. 1994); *Remand Order*, 9 FCC Rcd. 5,154 (1994), remanded for consideration of 1996 Act, Pacific Bell v. FCC, 81 F.3d 1147 (D.C. Cir. 1996). Indeed, the FCC refused to act on an earlier CLEC petition for a collocation order until a number of major States had issued similar orders.

The FCC should use the States as laboratories, particularly on matters where a decision needs to be tailored to address local or regional circumstances. As they did in the past, a few States will make decisions that the FCC will regard as "good" and a few others will make "poor" decisions. Then it is likely that other States will copy and improve the "good" results and, when the evidence is clear and convincing, the FCC (or Congress) can quickly and confidently make national policy based on real-world experimental evidence (the best evidence) rather than on warring studies and sheer speculation about the future (the worst evidence). The result is less gridlock and fewer risky rolls of the regulatory dice.

### *E. Reduce Gridlock By Streamlining Remaining Regulatory Processes*

One cause of gridlock is that the regulatory process itself invites it. While some of the gridlock-inducing process is required by fundamental Constitutional requirements of due process and fairness, much of it is self-inflicted by regulators and regulatees. Consequently, many of the streamlining reforms could be implemented by the agencies rather than by legislation. However, to the extent that regulators are unwilling or unable to implement reforms, legislation can and should require them to do so.

It is important to understand that most State regulatory commissions aren't as gridlocked as the FCC. This observation leads to an obvious thought: could the FCC adopt any of the procedural techniques which seem to prevent gridlock at the State level? The chief distinguishing procedural difference between the FCC and State Commissions is that the FCC rarely holds contested evidentiary hearings while States generally rely on such trial-type hearings.

The FCC should use contested hearings before Administrative Law Judges ("ALJs") for fact-finding and adjudication instead of the current "paper hearing" processes. This recommendation is based on the successful process used in most, if not all, States. State proceedings often utilize a combination of paper filings (pre-filed testimony) and on-the-record hearings with cross-examination of witnesses before a hearing officer/administrative law judge or the Commissioners themselves. This can be quicker, less expensive, more transparent, and more sustainable[45]

45. The appellate judges are comfortable with and give credit to evidence tested during lower court trials. In contrast, they are likely to be more suspicious of evidence and decisions based on such "evidence" in the unfamiliar "paper proceedings" used by the FCC. As a result, the FCC's decisions are likely to get less Chevron deference from the Courts of Appeal. *See* Chevron U.S.A. v. Natural Res. Def. Council, 467 U.S. 837 (1984). This explanation for the FCC's rather poor appellate record has been advanced for many years in Telecommunications

than the current FCC process of relying exclusively on paper proceedings augmented by private lobbying.

The FCC currently has ALJs on its payroll,[46] but they aren't utilized: the ALJs' website indicates they issued just one three-page decision in 2005.[47] Greater utilization of ALJs is within the management purview of the FCC Chairman and would not require legislation (other than appropriations).

Another gridlock-reducing procedural change would be to reduce the number of Commissioners at the FCC from five to one. This would eliminate the process of having to find complex and often confusing compromises that are needed to get the votes of a majority of five Commissioners. Compromises, by their very nature, take time to develop, are less clear, and are less predictable. They are also more difficult to defend in appellate litigation, meaning that a compromise decision is often less final. A glaring example of this problem was the FCC's Triennial Review unbundling decision which featured six months of public wrangling among the Commissioners between the adoption of an Order at the FCC's monthly meeting and the release of the text of the Order.[48] The Commission's voluminous and complex Order was then vacated by an appeals court.[49]

The chief benefit of a multi-member regulatory commission is the natural check and balance of the compromise process. However, checks and balances can be achieved with other mechanisms. A short, renewable term for a single commissioner would keep the decision-maker on a short leash and provide a reasonable check and balance through the reappointment process. Judicial appeals of the single Commissioner's

---

Policy Review, a private Washington, DC-based weekly newsletter.

46. The FCC's website lists two ALJs with a staff of three assistants and describes their function as:

> The Office of Administrative Law Judges (OALJ) of the Federal Communications Commission is responsible for conducting the hearings ordered by the Commission. The hearing function includes acting on interlocutory requests filed in the proceedings such as petitions to intervene, petitions to enlarge issues, and contested discovery requests. An Administrative Law Judge, appointed under the APA, presides at the hearing during which documents and sworn testimony are received in evidence, and witnesses are cross-examined. At the conclusion of the evidentiary phase of a proceeding, the Presiding Administrative Law Judge writes and issues an Initial Decision which may be appealed to the Commission.

Federal Communications Commission, FCC Office of Administrative Law Judges, http://www.fcc.gov/oalj/ (last visited Mar. 26, 2006).

47. *Id.*

48. The FCC adopted the Order at a public session on February 20, 2003. The text of the Order was finally released on August 21, 2003, approximately six months later. *See Triennial Review Order*, *supra* note 20, at 6,978.

49. U.S. Telecom Ass'n v. FCC, 359 F.3d 554 (D.C. Cir. 2004).

decisions as well as the normal legislative oversight process also provide additional checks and balances.

There may be some concern that the FCC's regulation of mass media content is not suitable for a single decision-maker and should continue to be regulated by a multi-member Commission. This is a legitimate concern which could be addressed, for example, by splitting the "telecommunications" and "content" responsibilities, perhaps leaving content to a multi-member Commission like the current FCC and transferring telecommunications to a new agency headed by a single decision-maker.[50]

Gridlock can also be reduced by imposing meaningful penalties for dilatory abuse of process. Companies with great financial resources who desire to maintain the *status quo* can use those resources to support the endless proceedings and litigation which contribute to gridlock. Penalties for abusing the process need to be sufficiently large in relation to the abuser's resources that they would deter the abuse. As such, large companies would be subject to larger penalties than smaller companies. Legislation may be required to permit the imposition of substantial penalties.

Another means for reducing gridlock, this time at the judicial level, would be to require that all appeals of FCC decisions would be heard in the same court (presumably the D.C. Circuit). This would streamline the judicial process in two ways. First, it would eliminate the forum shopping that frequently accompanies the appeals of FCC decisions as different appellants seek to have appeals heard in different Circuit Courts of Appeals. Second, by designating one appeals court to hear all telecom cases, the Court will develop telecom expertise, resulting (hopefully) in quicker, more consistent, and better grounded decisions.

## III. ADAPTING TO CHANGE: REGULATION MUST ADAPT QUICKLY TO DIFFERENT AND CHANGING MARKET CIRCUMSTANCES

Because the technological and market changes affecting the broad telecommunications industry will happen at different times and at different speeds, and will go in different directions in different markets, the ideal government policy response will be tailored (and constantly re-tailored) to the particular circumstances of each market.

Managers, investors and users need to know quickly and with reasonable assurance what the government's rules and policies are going to be in each market so that they can adapt their activities accordingly. If

50. An obvious difficulty with that approach is that having two separate regulatory bodies would be somewhat inconsistent with the "convergence" that is blurring the distinction between "transmission" and "content."

the government policy or regulation doesn't precisely fit the ever-changing situation, the result is gridlock, as parties continually try to find a "one size fits all" solution, and suboptimal decisions, which harm consumers, investors, and the industry.

It is useful to remember that a principle rationale of regulation is to protect consumers from abuse by dominant suppliers of essential services. Therefore, determining what kind of regulation should be applied to which kind of service, and whether all services should be regulated identically, should be done from the perspective of consumers. Unfortunately, the perspective of consumers on these issues will depend largely on the specific circumstances of the market in which the consumer finds him or herself.

### *A. Circumstances Vary Widely By Geographic Market*

Consider, for example, the vastly different demographic circumstances of two Manhattans: the well-known one in New York and the virtually unknown one in Nevada.[51]

| | Manhattan, New York[52] | Manhattan, Nevada[53] |
|---|---|---|
| **Population** | 1,537,195 | 1,841 |
| **Area (sq. miles)** | 23 sq. mi. | 1,801 sq. mi. |
| **Population Density** | 66,940.1/sq. mi. | 1.02/sq. mi. |
| **Per Capita Income** | $42,922 | $20,881 |

Note: Data based on 2000 Census

51. According to the Manhattan, NV town librarian, the nearest grocery store is 25 miles in one direction and 50 in the other; the nearest Wal*Mart is 300 miles from the town. Telephone interview with Librarian, Manhattan Town Library, in Manhattan, Nev. (Apr. 2005);

> ". . . once a flourishing mining community of 30,000 people, Manhattan is now populated with vacation homes and just a sprinkle of year-round residents. The town of Manhattan sprang up, almost overnight, in 1905, after a ranch hand named Humphrey discovered gold during his lunch break. . .There have been a few other mining operations in recent years, and a small number of people make their home in Manhattan today. There is a post office and public library, as well as one or two bars open for business. . .the landscape still contains old mining artifacts scattered here and there. The surrounding countryside is attractive, with rough hillsides and forests of juniper and pinion trees. Manhattan and the surrounding area is a great destination for sightseers and history buffs."

Mountainsage.org, Belmont, *available at* http://www.mountainsage.org/Belmont.htm (last visited Mar. 25, 2006).

52. U.S. CENSUS BUREAU, UNITED STATES CENSUS 2000 SUMMARY FILE 3 (2002), *available at* http://www2.census.gov/census_2000/datasets/Summary_File_3/.

53. *Id.*

In addition to these demographic differences—and probably because of them—the residents of the two Manhattans enjoy vastly different telecommunications circumstances.

| | Manhattan, New York | Manhattan, Nevada |
|---|---|---|
| ILEC (market cap[54]) | Verizon ($89B) | Citizens ($4.1B) |
| CLECs[55] | 14-23 per Zip Code[56] | 0 |
| Cellphone Carriers | 4 nat'l + resellers | No service[57] |
| Cable Television | Ubiquitous | None[58] |
| Broadband service | 8-18 per Zip Code[59] | Satellite only[60] |
| Public WiFi[61] | 1,000+ | None |

Considering the vastly different circumstances of Manhattan, NY and Manhattan, NV, it is likely that a national telecommunications regulatory system that is reasonably well-suited to one would not be optimal for the other.[62] Every community in the United States,

54. Market cap (market capitalization) is based on the closing price of the company's stock multiplied by the number of outstanding shares. These market caps are as of January 13, 2006, as reported at http://finance.yahoo.com/.

55. Federal Commn'cs Comm'n, *Report*, http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/czip0604.pdf (last visited Mar. 25, 2006).

56. Manhattan, NY has 44 Zipcodes.

57. According to the Manhattan town librarian, the only place where "spotty" cellular phone service is available in Manhattan itself is at the library parking lot because the main highway, about five miles down the canyon, is visible from the there. The librarian explained that many residents of the town do have cellular phones for safety during the long drives, once they reach the highway. Interview with Librarian, *supra* note 52.

58. Telephone Interview with Operator, Nevada Cable Television Association, in Manhattan, Nev. (Apr. 2005). (stating that Manhattan, NV residents can get satellite TV and over-the-air television. ABC, CBS and NBC –and sometimes Fox–channels relayed from Reno and Las Vegas).

59. Federal Commn'cs Comm'n, *Report*, http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/hzip0604.pdf (last visited Mar. 25, 2006).

60. Since there is no cable TV service, there is no cable modem service. Telephone Interview with Nevada Cable Television Association, *supra* note 58. A telephone company Customer Service representative stated that Citizens does not offer DSL broadband service in Manhattan, NV and that there are no plans to do so. Telephone interview, April 2005. According to the town librarian, a few Manhattan, NV residents do have satellite data service and the library itself is considering satellite data service. However, such services tend to be very expensive compared to DSL or cable modem broadband and are not suitable for VoIP due to propagation delays. Telephone Interview with Librarian, *supra* note 51.

61. CNET, Hot Spot Zone, *at* http://reviews.cnet.com/4520-6659_7-726628-1.html?tag=fs. (last visited Mar. 26, 2006).

62. For example, because consumers in Manhattan, NY have a wide range of competitive choices for their basic telephone service, little or no retail regulation is needed for consumer protection. By contrast, consumers in Manhattan, NV have no practical choice with respect to telephone services so it is likely that some form of economic regulation will be needed for the

including three other Manhattans (in Montana, Illinois and Kansas), have their own unique demographic and telecom circumstances that will lie somewhere between the extremes of Manhattan, New York and Manhattan, Nevada. It is not likely that a regulatory system that is ideal for one community will be optimal for any other.

### *B. Circumstances May Change Substantially Over Time*

In addition to vastly different circumstances in each community at any given instant, the circumstances of each community are also changing constantly so that an optimal regulatory system will become suboptimal and possibly harmful if it does not adapt to the constantly changing circumstances.

How effective would a regulatory system be if it is predicated on the existence of vigorous marketplace competition but such competition does not develop (as seems likely in Manhattan, NV) or a once-competitive market become substantially less competitive due to bankruptcies, mergers, and consolidations (as could happen in Manhattan, NY)?

Consider a key question for forward-looking policymaking: Are multiple broadband infrastructures sustainable in *every* market? While multiple broadband systems may be sustainable in many markets, it is at least equally likely that the future structure of the telecommunications industry will be monopoly or oligopoly.[63] For example, in the absence of government intervention, the consolidation process that is well underway in the telephone, cable TV, and wireless industries could result in two infrastructures in many markets: one fiber-based "fat pipe" to every home and business for video and data services (with telephone being a VoIP data application)[64] and one wireless system providing "thinner pipes" for mobile and nomadic services. In very small markets such as Manhattan, NV, a single wireless broadband system may suffice for all applications, including video.

A regulatory system that assumes that the equilibrium state of the telecom industry is intense competition among multiple infrastructures will clearly be suboptimal—and perhaps totally ineffective—if the industry settles into a monopoly or duopoly structure.

It is impossible to predict the direction and pace of future evolution of the telecom industry in any market, never mind every market.

---

foreseeable future.

63. Eli Noam, *Broadband and Wireless: The Next Telecom Crises*, in THE FUTURE OF TELECOMMUNICATIONS INDUSTRIES, (Arnold Picot, ed., forthcoming Apr. 2006), *available at* http://www.citi.columbia.edu/elinoam/articles/Noam_NextTelecomCrisis_2005

64. If the economics of a market dictate that it can only sustain one profitable fiber-based network, then either the traditional "telco" or the "cable company" (or both) would eventually have to exit the market.

Therefore, a "future-proof" regulatory system cannot be predicated on any particular set of circumstances or evolutionary expectation.

Why should any community be condemned to a suboptimal regulatory system and to the suboptimal telecom service that flows from suboptimal regulation? Wouldn't it be better to have a system where the kind and degree of regulation is dynamically and constantly adapting to the changing circumstances of each market? Such a system of circumstantial regulation is more likely to produce results that are always closer to the optimal for each market than a static, one-size-fits-all approach.

Of course, it is easy to suggest that regulation should be optimized for and be responsive to the circumstances of each market. But is such a system really practical and feasible? How will it work? Won't it be chaotic? Won't there be less regulatory certainty? Won't it be difficult?

For purposes of this article, it is sufficient to note that the current system doesn't seem to be working very effectively and one reason is that it is too uniform, too static, and too rigid. Perhaps it is simply time to try circumstantial regulation—that is, a flexible, adaptable, dynamic system—instead of tinkering with "one size fits all" regulation in the expectation that it can be made to work better. With circumstantial regulation the kind and degree of regulation will dynamically and constantly adapt to the changing circumstances of each market so that there would be a greater chance that regulation would be more optimal for every market.

As noted previously in this article, "muddling through" by State Commissions is one form of circumstantial regulation which would result in better, less risky, and more sustainable decisions.[65] One reason that "muddling through" by the States is less risky is that a Federal policy can never be optimal in all markets across this diverse nation. Policies that benefit the low density rural states, for example, may disadvantage the densely populated states, and *vice versa*. "Muddling through" in the States also reduces regulatory and financial risk by allowing for a continuous and low-risk iterative process of field experimentation, testing, and fine tuning of business strategies and public policies before irrevocable, major investment bets are placed. This was how local competition was developing before the Telecom Act upset the process.[66]

The regulatory system established by the 1934 and 1996 Acts inhibits the granular experimentation that could reduce risk in a dynamic industry and can make regulatory responses to industry problems faster and more effective. When the FCC attempted to delegate some decision-making to the States in its third attempt to define the network

65. *Supra* notes 43 and 44 and accompanying text.
66. *Supra* note 43 and accompanying text.

elements that should be unbundled as a result of the "necessary and impair" standard established by the Telecom Act,[67] the Commission's decision was overturned by the DC Circuit Court as an improper delegation of its authority.[68] Therefore, a statutory change may be needed to allow the circumstantial regulation that will produce more optimal results in every market. Congress should include in any new telecom law a provision that clearly empowers the FCC to delegate its authority to the States and to enlist the States in experiments.[69]

## IV. IF NEW LEGISLATION IS NEEDED, REPEAL THE 1934 ACT AND START FROM SCRATCH WITH A SIMPLE, ADAPTABLE LAW

There seems to be a growing consensus that the Communications Act of 1934 as amended by the Telecommunications Act of 1996 needs to be revised. Members of Congress, pundits, and industry leaders have, to varying degrees, called for substantial changes to the Communications Act, a number of bills have been introduced, and discussion drafts are circulating on Capitol Hill.

One major reason for the dissatisfaction is that the 1996 amendments were obsolete when they were enacted because of the rapid changes in telecom technology and the telecom industry. At best, the 1996 Act was backward-looking, attempting to fix problems that became apparent in the decade from 1985-95. Whether or not the fixes were successful is debatable. But it is clear that the Act was not forward-looking and therefore did not (and perhaps could not) foresee the rapid evolution of the Internet and broadband communications, the displacement of wireline telephones by wireless, convergence of telecom and television, or the boom-bust-consolidation of the industry.

The 1996 Telecom Act was the product of at least 10 years of Congressional inquiry and activity. If the Pandora's Box of new legislation is opened in 2006-07, it must be closed as quickly as possible to prevent legislative uncertainty (a.k.a., gridlock) from further delaying the recovery of the telecom industry. Such delay would have adverse consequences for individual consumers as well as the United States' international competitiveness and overall economic growth.

Quick legislation means very simple and very short legislation. This also argues against attempting to amend the current law since the amending process will encourage every faction to try to preserve its special privileges— a sure recipe for legislative gridlock. Finally, to avoid the fast obsolescence that plagued the '96 act, a new telecom statute

67. Triennial Review Order, *supra* note 20, at 17,094.

68. *See* U.S. Telecomm. Ass'n, 359 F.3d at 554.

69. A similar proposal is included in the proposed Digital Age Communications Act, *supra* note 25.

should not try to micromanage and it must not embed into law a static view of technology, the industry, or the market. Rather, a new law should allow telecom regulation to be tailored and re-tailored to the specific and constantly changing circumstances of each market.

To minimize legislative gridlock and to produce a "future-proof" law with lasting utility, a new telecom statute should focus almost exclusively on two subjects: *principles* that most stakeholders can support, so that regulators (and reviewing courts) are clear about the statutory goals and objectives; and *processes*, so that final, clear, and sustainable decisions can be reached in a short period of time.

Conversely, any new statute should NOT deal with "substance" in the sense of embodying in law Congressional micromanagement of the telecom industry, particularly to resolve current industry disputes or to specify a particular regulatory policy. Any such embodiment is likely to be wrong or obsolete or both.

### *A. Principles for a New Telecom Law*

A new statute should begin with a clear and concise statement of the fundamental goal of the law, perhaps modeled on the similar provisions of the current Communications Act. Sample language may include the following:

> The purpose of this law is to establish and maintain an efficient and reliable nationwide and worldwide telecommunications system capable of providing all persons with access to affordable telecommunications services. The Commission hereby established shall rely, wherever reasonably feasible, on competitive market forces to achieve this purpose and shall regulate telecommunications services and facilities in each market only to the extent and only for so long as market forces are insufficient to achieve this purpose or are unable to prevent the abuse of consumers.

Next, an obsolescence-proof law will need to define "telecommunications" and "telecommunications service" very broadly so that it is technology-neutral and can accommodate rapid and unknown technological developments for decades. A new telecommunications statute should then empower and require the federal regulator (the Commission) to follow broadly written principles, such as those summarized in the following paragraphs. Competition is to be the preferred means in every market for encouraging fair prices, innovation, and efficiency.

To encourage competitive markets, networks must interconnect with each other upon request at any technically feasible location on commercially reasonable terms and conditions and consumers may attach

any devices to the network and use telecommunications services without restriction provided they cause no harm to the networks.

Where competition is demonstrated to be insufficient to achieve the statute's goals, regulation should be applied on a geographically granular basis to the minimum extent required to achieve the statute's purpose or to protect consumers from pricing and service abuses. Geographically granular regulation should be regularly reviewed and adjusted to accommodate the changing circumstances of each market, reduced or eliminated if there is less or no need, and increased if there is a greater need.

The Federal government has plenary authority over all telecommunications facilities and services. However, the Federal authority shall be delegated broadly to State commissions when the varying circumstances of each locality or region require varying regulatory responses or policies. The delegation to the States must include the directives and decisional standards needed to comply with Constitutional requirements and in most cases the Federal Commission would hear initial appeals of decisions made by State regulators pursuant to delegated authority.

States may exercise authority, particularly traditional police powers, over telecommunications, telecommunication facilities, and telecommunications services, provided that such exercise does not conflict with Federal law, policy, or regulations. The Federal Commission or courts shall preempt any conflicting State action.

The Federal Commission may conduct experiments of limited geographic scope and shall generally encourage States to experiment with regulatory policies by, *inter alia*, forbearing from applying Federal laws or regulations that conflict with a State's experiment. A State may petition the Commission for authority to conduct a regulatory experiment of up to two years duration, including any necessary forbearance. Unless the Commission denies the petition within 60 days, the petition shall be deemed granted. The best evidence in proceedings before the Federal regulator or other States is the results of relevant State or Federal experiments.

Neither Federal nor State regulators shall regulate the price, quality, or other characteristics of retail telecommunications services (those predominantly utilized by individual consumers) in the absence of demonstrated abuse of consumers. States have the initial responsibility for determining the existence of consumer abuse and for determining and applying the least regulation required to eliminate the abuse. The Federal Commission would act if States refused to consider petitions alleging consumer abuse. The Federal Commission may issue standards and guidelines for the States to apply in determining the existence of a

consumer abuse and for the regulation of abuses. The Federal Commission will hear appeals from State decisions to determine abuse and to regulate or to not regulate as a result.

All carrier-to-carrier issues (including but not limited to such matters as collocation, access charges, reciprocal compensation, performance standards, and all other interconnection matters) shall be resolved exclusively by bilateral negotiation and commercial arbitration.

The Commission shall allocate and assign all radio frequency spectrum not controlled by the Federal government for government use in the manner it deems most efficient and equitable. Regulators shall be prohibited from requiring telecommunications service providers to be involved in collecting or contributing funds to support universal service, and regulators shall not impose any implicit subsidies in any rate regulation.[70] The Commission may, after due process, revoke a service provider's operating, radio frequency or other licenses and authorizations for activities that constitute systemic untrustworthiness and may prohibit licensees from employing as managers persons who have a record of untrustworthiness in the telecom business.

### *B. Process and Procedures to Be Included in a New Telecom Law*

After stating the broad objectives and principles, the telecom law should then specify process and procedures to be followed by the regulators to achieve the goals. The process and procedure should be simple and streamlined so as to minimize gridlock, expense and uncertainty. The following paragraphs provide some summary examples.

Federal and State regulators shall forebear from applying any statutory provision for entire geographic markets and all services, or on a more granular market-by-market, service-by-service basis, if they determine that such forbearance is likely to better achieve the statute's objectives than regulation.

The federal regulator will be a single Commissioner appointed by the President and confirmed by the Senate for two year renewable terms.

---

70. Ideally, other legislation will deal with the important Universal Service issue. However, a new telecom statute could provide for a non-regulatory mechanism to support Universal Service. One approach would be that individuals eligible for the Department of Agriculture's food stamp program would also receive a telecom stamp from DoA. The dollar amount of the telecom stamp would be the difference between the unregulated retail rate for basic telephone service provided by the largest provider of service in the market (zip code?) and 115% of the national average retail price for such service. The telecom company providing the service selected by the consumer would redeem the stamp from DoA. Telecom stamps should be funded from: a) the 3% telephone excise tax (which shall not be increased); and b) if necessary, general revenues. *See also* the similar proposal provided by the author included as an appendix to the report of the DACA Universal Service Working Group. http://www.pff.org/issues-pubs/books/051207daca-usf-2.0.pdf.

All adjudicatory proceedings before the federal agency shall be conducted by Administrative Law Judges except where the Commissioner determines on a case-by-case basis that another process would be more efficient, fair and transparent. All appeals of the Commission's decisions will be made to the Court of Appeals for the District of Columbia Circuit. State decisions administering Federal statutes are to be appealed to an appropriate Federal District Court.

With respect to service provider interconnection arrangements, all matters not resolved through bilateral negotiations shall be resolved by a State Commission Order drafted by a commercial arbitrator and adopted by the Commission. Parties to the arbitration may agree to any commercial arbitration procedure, but "baseball" arbitration (where the arbitrator many only select the entirety of one of the party's best and final package of offers regarding all the unresolved issues) will be the default arbitration process. Parties can agree that an arbitration result will apply only to specified markets within a State or to any number of specified States but a state-wide scope will be the default.

The arbitration decision will be submitted to the affected State Commission for ratification and the State must accord the arbitration result substantial weight, with the opponent of the arbitration decision having the burden of demonstrating that, overall, the arbitration decision is inconsistent with law, Federal policies, or is likely to lead to significant harm to public interest. Where the arbitration covers more than one State, an *ad hoc* panel composed of one State Commissioner selected by a majority of the State Commissioners from each affected State will consider the ratification and the majority decision of the *ad hoc* panel will bind all affected States. If it does not ratify the arbitrator's decision, the State Commission's or *ad hoc* panel's only recourse is to order another arbitration. "Opt-in" or "all-or-nothing" would be available for similarly situated service providers that choose to avoid negotiation.

## CONCLUSION

The current system for regulating telecommunications has two serious and related failings: it is unable to adapt quickly to the rapid changes in technology, business conditions, and market demands; and, it is unable to adapt with sufficient precision to the widely varying circumstances of each market. The result is that the current regulatory system fails both consumers and the telecom industry. Because the telecommunications-information industry plays such a major role in society and in every sort of business enterprise, suboptimal performance of the regulatory system adversely affects the entire nation.

These twin failings can be remedied. Regulators can act within existing laws to reduce some of the gridlock by reforming their practices

and procedures. However, other changes, particularly those that would encourage flexible and adaptive circumstantial regulation, probably require new legislation.

Trying to solve these problems by amending the existing law is likely to cause years of legislative gridlock and produce another complex, unsatisfactory and static compromise similar to the Telecommunications Act of 1996. A better approach for the 21st century would be to start at the beginning with a simple, short new statute that establishes broad policy goals and provides for flexible procedures and processes when regulation is required.

# NATIONAL SECURITY ON THE LINE

SUSAN LANDAU*



## INTRODUCTION[1]

Wiretaps have been used by United States law enforcement for well over a century.[2] However, with the exception of a brief period during the First World War,[3] not until the 1960s did Congress pass the first federal statute governing their use. Title III of the 1968 Omnibus Crime Control and Safe Streets Act,[4] which regulated the use of wiretaps in criminal investigations, was followed by the 1978 Foreign Intelligence

* Susan Landau, Distinguished Engineer, Sun Microsystems. Email: susan.landau@sun.com. My work on this article has greatly benefited from the comments of Yochai Benkler, Whitfield Diffie, Michael Froomkin, Marc Rotenberg, and Roland Trope.

1. This article is based on Susan Landau, *Security, Wiretapping, and the Internet*, IEEE SECURITY AND PRIVACY, 26-33 (Nov./Dec. 2005). 2005 IEEE.

2. SAMUEL DASH, THE EAVESDROPPERS 23 (1959).

3. The Anti-Wiretap Statute (40 Stat. 1017, 1918) was in effect during the latter part of the war to prevent enemy agents from wiretapping.

4. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2521 (1968).

Surveillance Act,[5] which regulated the use of wiretaps in foreign-intelligence investigations. As telecommunications technology changed, law enforcement sought to keep the law current, and the Electronic Communications Privacy Act[6] and the controversial Communications Assistance for Law Enforcement Act (CALEA)[7] were passed.

In requiring that digitally-switched telephone networks be designed in accordance with federally-specified wiretapping standards, CALEA substantively changed the way telecommunications equipment was developed and deployed. Disagreements between the telephone companies and the Federal Bureau of Investigation (FBI), which had been charged with developing the CALEA standards, made implementation of the 1994 law exceptionally difficult. As a result, the Federal Communications Commission (FCC) delayed required implementation two years.

In 2004, the FBI petitioned the FCC to extend CALEA to Voice over IP (VoIP), meaning voice communications over the Internet (or using Internet protocols). CALEA, which placed law enforcement in the middle of the design process of communications technology, represented a fundamental alteration in the wiretapping laws established by Title III and FISA, and the result has been a chaotic and difficult implementation process. Because of the different architectures of the telephone and Internet networks, implementing CALEA on VoIP is likely to be even more difficult than implementing CALEA on telephony networks.[8] It not only poses risks to the U.S. economy (the potential loss of corporate information), but also to the freedom of U.S. citizens, and to U.S. national security (through the enabling of cost-effective massive intelligence gathering). This article focuses on those threats posed to national security though the reader should be aware of other objections to the FBI proposal, including concerns about threats to innovation and to civil liberties.[9] The issue of CALEA and VoIP is not the first time that conflict has arisen between the needs of law enforcement and the interests of national security in communications

5. 50 U.S.C. § 1801 (2006).

6. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

7. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994).

8. *See, e.g.,* IAB and IESG, RFC2804 — IETF Policy on Wiretapping (May 2000), http://www.rfc-archive.org/getrfc.php? rfc=2804.

9. *See, e.g.,* Joint Reply Comments of 8X8 Inc. et al., to the Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (Dec. 21, 2004), *available at* http://www.cdt.org/digi_tele/20041221joint.pdf; Joint Reply Comments of 8X8 Inc. et al., to the Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (Nov. 8, 2004), *available at* http://www.cdt.org/digi_tele/20041108indpubint.pdf.

infrastructure. In many ways, the fight over implementing CALEA in VoIP is reminiscent of the battles over the use of strong encryption during the 1990s, the "Crypto Wars."[10] Just as now, in the Crypto Wars, there were disputes about threats to innovation and civil liberties. Ultimately national security concerns, which include the need for good methods to ensure information security, carried the day. As a result, strong encryption is deployed throughout the infrastructure, despite the difficulties that the availability of strong encryption may pose for some national security and law enforcement investigations

CALEA requires building wiretapping capabilities into communications networks. The same issues are in play in CALEA applied to VoIP as existed in the Crypto Wars: although law enforcement has investigatory reasons for seeking to apply CALEA to VoIP, the national security requirements for information protection should be paramount. These argue against building an architected security breach into the communications network such as CALEA would require.

Understanding the issues raised when CALEA is applied to VoIP requires knowledge of a number of disparate areas. Part I traces the history of U.S. wiretap law, demonstrating what an abrupt change CALEA represents in wiretapping law. The problems that ensue when placing a law enforcement agency in charge of designing telephony standards are illustrated in Part II by tracing the history of CALEA. Indeed, the difficulties are compounded by applying CALEA to VoIP, because VoIP travels on a packet-switched network. Part III explains how the architecture of the Internet causes that network to be easier to subvert than circuit-switched networks. Through examining current reliance on the Internet as well as future dependencies created the by "billions and billions of devices" that will be connected to the Internet, Part IV presents the security threats that result from building surveillance tools into Internet communications protocols.

Investigating terrorist cases involve unusual techniques and require enrolling the "community." Part V analyzes the policy issues surrounding communications surveillance and terrorism investigations, and demonstrates that the law enforcement approach is counter-productive. The article concludes with an observation that CALEA, which forces surveillance capabilities into communications networks, represents a turnaround in U.S. policy of protection of communications privacy, a policy begun in the 1790s.

CALEA represents a sharp break with U.S. wiretap law. Its application to Voice over IP creates numerous security vulnerabilities.

10. *See, e.g.*, STEPHEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE (2001).

Security requirements should be, "First, do no harm." CALEA applied to VoIP does not pass this test and should not be approved.

## I. FEDERAL WIRETAPPING LAWS: A SHORT HISTORY

In putting the FBI into the role of designing wiretapping standards,[11] CALEA altered previous wiretap law, which proscribed rules governing the "tapper."[12] A brief history of U.S. wiretap law illuminates how anomalous CALEA is.

Except for a brief time during the First World War,[13] the first federal wiretap law appeared in 1967, in response to the *Katz*[14] case. The Supreme Court has ruled warrantless electronic bugging[15] illegal, establishing the doctrine of "legitimate expectation of privacy."[16]

Charles Katz was a gambler. Through an electronic bug put on a Los Angeles public phone booth, law-enforcement agents recorded Katz placing bets, in violation of Federal statutes prohibiting interstate gambling.[17] The Court ruled the law-enforcement bugging illegal. The Court found there is an expectation of privacy from even so public a place as a phone booth, and the warrantless bugs violated Katz's privacy. If there was to be electronic surveillance, a procedure for obtaining warrants needed to be enacted, spurring Congress to take action to regulate electronic surveillance.

The ensuing debate on wiretapping occurred during a period of social turmoil. The civil rights protests brought thousands of (non-violent) marchers to Washington; the opposition to the Vietnam War was about to do the same. The 1960s also saw the assassination of several of America's prominent leaders: President Kennedy, Malcolm X, Martin Luther King, and Senator Robert Kennedy. Into this context came the

---

11. CALEA, §§ 103, 107, (N.B. The law specifies the Attorney General will determine the standards issues, but that was understood during negotiations on the bill to actually mean the F.B.I.).

12. 18 U.S.C. §2518(4)(e) (2000). "An order authorizing the interception . . . shall . . . direct that a provider of a wire or electronic communication service . . . shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception . . . ."

13. Concern about enemy agents led to the federal Anti-Wiretap Statute.

14. Katz v. United States, 389 U.S. 347 (1967).

15. An electronic bug is a concealed microphone that operates by sending the signal through radio waves to the receiver, while a wiretap is a similar device that is connected to a communications circuit, such as the telephone network or the Internet, with the transmission being intercepted through the communications circuit itself.

16. The Katz decision did not use the expression "legitimate expectation of privacy," but in Smith v. Maryland, 442 U.S. 735, 740 (1979), the Court described the decision that way writing, "[c]onsistently with *Katz*. . . the application of the Fourth Amendment depends on whether the person . . . can claim . . . a 'legitimate expectation of privacy' . . . ."

17. Katz, 389 U.S. at 348.

findings of the 1967 President's commission on organized crime.[18]

Organized crime – widespread crime controlled through a centralized organization – was largely ignored by U.S. law enforcement (especially the FBI) until it was made quite public by the combination of the accidental discovery in 1959 of a meeting of crime bosses in upstate New York[19] and the testimony in 1963 of organized crime member Joseph Valachi to a Senate committee. With the lawbreakers' reliance on "victimless" crimes and its corruption of local law enforcement, organized crime is particularly difficult to investigate. The President's commission concluded that wiretapping was needed to break the back of organized crime. But even amongst law enforcement, there was not universal agreement with the commission.

Attorney General Ramsey Clark had prohibited federal law-enforcement use of wiretaps. The Chief Judge of the US District Court in Northern Illinois had testified to Congress that wiretaps were the mark of lazy investigators.[20] In a 1961 survey, attorneys general from California, Delaware, Missouri and New Mexico opposed federal wiretapping law.[21] Even President Johnson spoke against wiretapping.[22]

As Justice Louis Brandeis observed in his famous dissent in *Olmstead*,[23]

> [w]hen the Fourth and Fifth Amendments were adopted, 'the form that evil had heretofore taken' had been necessarily simple. Force and violence were then the only means known to man by which a government could directly impel self-incrimination . . . . But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in

18. President's Commissions on Law Enforcement, *The Challenge of Crime in a Free Society* (1967).

19. On November 15, 1957, a New York state patrolman in the "southern tier" of the state, near Pennsylvania, came upon a meeting of organized-crime bosses. The patrolman set up a roadblock, resulting in the identification of sixty-seven people. *See e.g.*, WHITFIELD DIFFIE AND SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998) at 168-69.

20. "In every case I know of where wiretapping has been used, the case could have been made without the use of the wiretap. Wiretapping in my opinion is mainly a crutch or shortcut used by inefficient or lazy investigators." S. REP. NO. 99-1097, at 1495 (1968).

21. *Wiretapping and Eavesdropping Legislation: Hearings on S. 1086, S. 1221, S. 1495, and S. 1822 Before the Subcomm. On Constitutional Rights*, 87th Cong. 545, 547, 554, 560 (1961).

22. 26 CONG. Q. WKLY. 1842 (July 19, 1968).

23. Olmstead v. United States, 277 U.S. 438, 473-76 (1928) (Brandeis, J., dissenting).

> court of what is whispered in the closet . . . . Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard . . . As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.[24]

Experience had already shown that, just as Justice Brandeis has predicted, wiretapping is a broad form of investigatory search. Congress was well aware that the FBI's warrantless wiretapping had extended to members of the government; from the Truman era through the Nixon presidency, the FBI had wiretapped on Supreme Court Justices, Congressional staff, and other members of the government.[25] Nonetheless the Omnibus Crime Control and Safe Streets Act of 1968,[26] Title III of which established the basic law for interceptions performed in criminal investigations, was made law.[27] Because of concern over the intrusiveness of electronic surveillance searches, Title III tightly controlled their use.

The presidential commission recommended that law-enforcement wiretapping be limited to investigations of serious crimes and that a wiretap warrant be obtained only after a set of stringent requirements were met. Congress established these controls over law-enforcement wiretapping, as well as a public reporting mechanism, the *Wiretap Report,* published annually by the Administrative Office of the U.S. Courts. Title III was limited to wiretap warrants for investigations of criminal cases – but criminal investigations are only part of the wiretapping equation.

After *Katz*, warrantless electronic surveillance continued to be used for what were characterized as domestic "national security" cases. Then in 1972, the Supreme Court, ruled that "the constitutional basis of the President's domestic security role . . . must be exercised in a manner compatible with the Fourth Amendment."[28] The Court invited Congress to rectify the situation by establishing procedures for national-security wiretaps. Because of Watergate,[29] the process took half-a-dozen years.

---

24. *Id.*

25. *See, i.e.*, ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT*,* 25 (1992); INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT, BOOK III, S. REP. NO. 94-755, at 309 (1976).

26. 18 U.S.C. §§ 2510–2521 (1968).

27. These include §§2516-2519 of Title III.

28. United States v. Dist. Ct., 407 U.S. 297, 320 (1972).

29. "Watergate" refers to the 1972 burglary of the Democratic Party National Committee

The third-rate burglary[30] that brought down the presidency revealed widespread political wiretapping under the guise of national security investigations. The involvement of many of the intelligence agencies in surveillance activities caused great concern. In January 1975, the Senate appointed an eleven-member special committee to determine the extent to which "illegal, improper, or unethical" intelligence activities were engaged in by government agencies.[31] Thus was created the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the Church Committee after its chair, Senator Frank Church. The Church Committee uncovered decades of government surveillance of what should have been protected political activity. Beginning its study with 1936, the Church Committee worked its way through a forty-year history of surveillance of, among others, ordinary citizens engaged in political activity, Congressional staff, Federal judges, and political activists. Neither party nor any President was immune to the temptation of electronic surveillance – wiretaps and bugs – used for political purposes.

Harry Truman wiretapped the Washington lobbyist (and FDR confidant) Thomas Corcoran. John F. Kennedy, during negotiations with Congress about sugar tariffs, acceded to tapping of Congressional staff. Kennedy and Lyndon Johnson both allowed the FBI electronic surveillance of Martin Luther King, Jr. During the 1968 Presidential race, Johnson arranged for the wiretapping of his own Vice President, Hubert Humphrey. Richard Nixon had tapped members of his staff, former members of his staff, the press, his political opposition, and ordinary citizens engaged in protected First Amendment activities.

The hearings revealed numerous illegal covert operations by the intelligence agencies, and the Church Committee concluded with a series of quite specific recommendations designed to protect the security and privacy of Americans:

o Recommendation 6: The CIA should not conduct electronic surveillance, unauthorized entry, or mail opening within the United States for any purpose.[32]

o Recommendation 15: NSA should take all practicable measures

---

offices at the Watergate complex in Washington by five men in the pay of the Republican Committee to Re-elect the President. Two years of investigations revealed extensive political spying and a cover up of the Watergate break-in by high government officials, including the President. President Nixon resigned, the first president ever to do so. *See, e.g.*, CARL BERNSTEIN AND BOB WOODWARD, ALL THE PRESIDENT'S MEN (1974).

30. This was how the Watergate break-in was originally characterized by Ron Ziegler, White House Press Secretary.

31. S. RES. 21, 94th Cong. (1975).

32. S. REP. NO. 94-755, at 302 (1976).

consistent with its foreign intelligence mission to eliminate or minimize the interception, selection, and monitoring of communications of Americans from the foreign communications.[33]

o Recommendation 16: NSA should not be permitted to select for monitoring any communication to, from, or about an American without his consent, except for the purpose of obtaining information about hostile foreign intelligence or terrorist activities, and then only if a warrant approving such monitoring is obtained in accordance with procedures similar to those contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[34]

o Recommendation 52: All non-consensual electronic surveillance should be conducted to judicial warrants issued under authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

The Act should be amended to provide, with respect to electronic surveillance of foreigners in the United States, that a warrant may issue if:

(a) There is probable cause that the target is an officer, employee, or conscious agent of a foreign power.

(b) The Attorney General has certified that the surveillance is likely to reveal information necessary to the protection of the nation against actual or potential attack or other hostile acts of force of a foreign power; to obtain foreign intelligence deemed essential to the security of the United States; or to protect national security information against hostile foreign intelligence activity.

(c) With respect to any such electronic surveillance, the judge should adopt procedures to minimize the acquisition and retention of non-foreign intelligence information about Americans.

(d) Such electronic surveillance should be exempt from the disclosure requirements of Title III of the 1968 Act as to foreigners generally and as to Americans if they are involved in hostile foreign intelligence activity (except where disclosure is called for in connection with the defense in the case of criminal prosecution.[35]

Based on the Church Committee's recommendations, the Foreign Intelligence Surveillance Act (FISA) became law in 1978.

Throughout this fifty-year history, from *Olmstead* to FISA, the central issue surrounding wiretapping was under what circumstances government agents would be permitted to wiretap. Title III and FISA struck a balance between law enforcement and civil liberties on electronic surveillance. Over the years, the balance has shifted some in the direction of law enforcement. First, the number of crimes subject to an

33. *Id.* at 309.
34. *Id.*
35. *Id.* at 327–28.

electronic surveillance order has gone from the original twenty-six in Title III to just under a hundred today.[36] Additionally, under the Electronic Communications Privacy Act,[37] pen registers and trap-and-trace devices, which record incoming and outgoing calls on a phone line, became obtainable under a subpoena.[38] Because the purpose of FISA was the collection of foreign intelligence, the requirements for an electronic surveillance order were looser than those of Title III, requiring only that the "target be a foreign power or an agent of a foreign power"[39] rather than the more restrictive "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense [enumerated elsewhere]."[40] For over two decades, FISA was limited to gathering foreign intelligence, but the Patriot Act changed the requirement on FISA from foreign intelligence being the "primary purpose" of the surveillance, to foreign intelligence being only a "significant purpose".[41] These changes, especially the diminution of the "wall" between Title III and FISA, are major ones, and have been the subject of serious discussion and analysis.[42]

Yet until CALEA, wiretap law did not delve into how the telephone networks should be configured. In each instance, wiretap law focused on what could be obtained and how law enforcement should obtain it (e.g., a subpoena in the case of a pen register or trap-and-trace order). In no instance prior to CALEA did Congress legislate how the communications providers should configure their networks; instead, Congress left the design of wiretap technology to the people who developed and ran the communications technology.

Leaving discretion about the architecture of the telephone network to the providers makes a great deal of sense. The telephone companies were required by law to satisfy the needs of law enforcement; at the same time, market forces make the privacy needs of their customers important to the company. So the telephone companies are in a natural position to balance the opposing needs of law enforcement and customer privacy. As a law enforcement agency situated in the executive branch, the FBI lacks a direct constituency that might demand protections for

36. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 1 (1997), *available at* http://www.cdt.org/publications/lawreview/1997albany.shtml).

37. Pub. L. No. 99-508.

38. 18 U.S.C. §§ 3121-3127 (2001).

39. 18 U.S.C. § 1804 (2006).

40. 18 U.S.C. § 2518 (1998).

41. USA Patriot Act, 115 Stat. 272 (codified at 50 U.S.C. §1804(a)(7)(B).

42. *See, e.g.,* Daniel J. Solove, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance Law: Reshaping the Framework: Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2004).

communications privacy. By establishing the FBI[43] as the arbiter of the standards for wiretap-enabled digitally-switched telephony, CALEA eliminated the delicate balance that Title III and FISA had established between the competing needs of law enforcement and citizenry privacy rights.

With the advent of VoIP, the changes wrought by CALEA created not only privacy concerns but also security implications. CALEA requires an architected security breach in the communications network. The FBI's focus on solving cases and establishing a "chain of evidence" has caused the bureau to emphasize one set of issues—catching and convicting criminals —over another—securing U.S. communications. Indeed, CALEA requires an architected security breach in the communications network. The FBI's actions pursuant to CALEA impede the building of security protections into communications networks, an issue examined in the next section.

## II. EXTENDING CALEA — WHAT DOES LAW ENFORCEMENT WANT?

The AT&T break-up in 1984 created a new problem for law enforcement: a large variety of service providers and equipment manufacturers. Instead of negotiating with a single provider on the standards for implementing legally authorized wiretaps, law enforcement faced a plethora of new telecommunications market participants.[44] In the early 1990s, the FBI began making public statements about law enforcement's inability to complete "hundreds" of surveillance orders.[45] In Congressional testimony, citing an "informal" 1993 survey of federal, state, and local law enforcement agencies, FBI Director Freeh stated there were 91 instances of electronic surveillance court orders that law enforcement could not implement due to technological impediments.[46]

---

43. CALEA establishes that the "Attorney General, in coordination with other Federal, State, and local law enforcement agencies" shall determine the standards; it was understood during negotiations on the bill that the FBI would be the actual agency determining the standards. 47 U.S.C. §1006(a)(1) (2006).

44. According to FBI testimony, by 1994 there were two thousand common carriers. Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Technology, Environment and Aviation of the H. Comm. on Science, Space, and Technology, 103rd Cong. 5 (1994) (statement of James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, FBI).

45. "The development of technology is moving so rapidly that several hundred court orders already have been prevented by new technological impediments associated with advanced communications equipment." Louis Freeh, FBI Director, Address Before the American Law Institute (May 19, 1994), in CRYPTOGRAPHY AND PRIVACY SOURCEBOOK (David Banisar ed., 1994).

46. Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomms. and Finance, H. Comm. on Energy and Commerce, 103rd Cong. 33 (1994) (testimony of Louis Freeh, FBI Director).

The public was not privy to the data leading to the conclusion that the nation's wiretapping laws needed an overhaul. When the survey information was finally made public in late 1994, the only data visible in the tables provided were the column headings and listings of the type of crimes being investigated[47] — everything else was blacked out. Without specific information about the difficulties law enforcement had encountered, it was impossible to determine how serious law enforcement wiretapping problems had actually been (and thus, by extension, the necessity for the new law). But that scarcely mattered: CALEA had already been enacted. Difficulties in its implementation were just beginning.

CALEA provided a "safe-harbor" provision, under which carriers that followed accepted industry standards would be considered in compliance with the law even if these carriers were actually unable to execute certain wiretaps.[48] There was, however, sharp disagreement over what constituted "accepted industry standards." During negotiations over the bill, the telephone companies had understood that accepted industry standards would be worked out jointly between industry and law enforcement, but after the law's passage, the FBI took the stance that it was in charge of setting these standards, called the "punch-list."

Civil-liberties groups and the telephone companies strongly objected to several of the proposed standards.[49] The ensuing controversy created considerable delays in carrying out the provisions of the Act. In response, Representative Bob Barr proposed the *CALEA Implementation Amendments of 1998*,[50] which would have delayed implementation of CALEA until October 1, 2000. Instead, the FCC stepped in and delayed required CALEA compliance to June 30, 2000.[51]

Meanwhile, the United States Telecommunications Association filed suit over aspects of "accepted" industry standards. One issue was

47. Sensitive Electronic Surveillance Techniques: Survey of Problems Encountered in Conducting Authorized Electronic Surveillance as Reported by FBI Field Offices, in 1995 EPIC Cryptography and Privacy Sourcebook: Documents on Encryption Policy, Wiretapping, and Information Warfare B 1-11 (1995).

48. CALEA (codified at 47 U.S.C. § 1006(a)(2) (2006)).

49. The FBI originally proposed a surveillance capacity of thirty-thousand simultaneous intercepts (wiretaps, pen registers, and/or trap-and-trace devices) at a time when the annual total of surveillances was less than a quarter that number. Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 199, 53643-53646 (Oct. 16, 1995). After great objections to the methodology used in arriving at this number, the FBI revised the capacity estimate using a different method that resulted in a requirement for the capacity of sixty-thousand simultaneous surveillances (or eight times the number of annual wiretaps, pen registers, and trap-and-trace devices in 1996). *See* Implications of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 9, 192 (Jan. 14. 1997).

50. H.R. REP. NO. 105-3221 (1998).

51. CALEA's original compliance date was October 25, 1998

extraction of *post-cut-through dialed digit* extraction – those digits sent *after* the initial connection. In old telephony systems, such digits did not exist; if a person wanted to access their checking account, for example, they had to speak to a person. Thus, if law enforcement wanted to record this communication, because it was part of a telephone conversation, law enforcement needed a wiretap warrant. But new technology has changed things. In modern punch-dial telephony systems, there is no person at the bank end of the call. Instead, the customer navigates to her account information through an automated phone menu. The FBI argued that since there was no conversation, such data should not be subject to a wiretap warrant, but instead could be released through a subpoena. The service providers disagreed.

Another contentious issue was location information. With fixed telephony systems, location information had not been an issue, but cell phones created a novel situation. During the CALEA hearings, FBI Director Louis Freeh had said that FBI would *not* require that call-identifying information, defined as "dialing or signaling information that identifies the origin, direction, destination, and termination of each communication", include location information.[52] Indeed CALEA is explicit on this issue: "call-identifying information . . .does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[53] However, once CALEA passed, the situation changed. The FBI included the location of the cellular antenna serving the call as part of the proposed CALEA standards for call-identifying information.

In *USTA v. FCC*, the D.C. Circuit affirmed a District Court ruling that the FCC incorrectly granted several of the FBI punch-list requirements.[54] Specifically, the court ruled that the post-cut-through digits could not be obtained solely through a pen-register subpoena, but instead required a wiretap order. However, the D.C. Circuit agreed with the FCC ruling that location of the cellular tower was to be disclosed

52. "[Call setup information] does not include any information which disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent, whatsoever, with reference to this term, to acquire anything that could properly be called 'tracking information.'" *Digital Telephony and Law Enforcement Access Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary,* 103rd Cong. 6 (1994) (statement of Louis Freeh). "Call setup information" was later changed to the term "call-identifying information, and that is the expression used in the law.

53. CALEA §103(a)(2)(B) (codified at 47 U.S.C. §1002).

54. 227 F.3d 450 (D.C. Cir. 2000).

with call-identifying information.[55] This yielded a brief period of peace that was quickly beset by a new set of issues.

In late 2003, the FBI gave notice to the FCC that the CALEA requirements should be extended to VoIP. This demand was controversial. CALEA has an exemption for "information services," a reference to the (nascent) Internet of 1994. Specifically, CALEA exempts "information services" from the common carriage requirements applying to telecommunications carriers.[56]

In its March 2004 petition to the FCC, the FBI declared that the ability of law enforcement to wiretap "is *being compromised today*,"[57] and the movement of voice calls to the Internet is already threatening law enforcement's capabilities to conduct electronic surveillance.[58] Despite the sweeping statement of "the serious impact" of the move to packet-based networks, however, no concrete evidence of actual failures of wiretapping VoIP were presented.[59] Indeed, a recent Inspector General report on CALEA implementation says quite the contrary.[60]

The FBI claimed that there was an ambiguity in the meaning of "telecommunications service" and requested that the Commission clarify which services and entities are subject to CALEA.[61] The Bureau also requested that the Commission establish benchmarks and deadlines for

---

55. *Id.*

56. CALEA §102(8)(A)(B)(C) (codified at 47 U.S.C. §1001).

57. Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, filed by the U.S. Department of Justice, the Federal Bureau of Investigation & the Drug Enforcement Administration, 8 (Mar.10, 2004).[hereinafter The Petition].

58. *Id.* at 27.

59. *Id.*

60. The Inspector General's report said that,

> The FBI provided a document entitled *FBI Investigative Technology Division CALEA Law Enforcement Case Examples* dated October 29. 2004. The document contained 23 examples of unsuccessful intercepts, none of which involved electronic surveillance for wireline intercepts. The 23 examples involved either wireless or Voice over Internet Protocol (VoIP), which seemed to be law enforcement's primary concern since a low percentage of wireline intercepts are conducted. In addition, we believe these examples are not necessarily indicative of technology that is negatively impacting law enforcement's ability to conduct electronic surveillance because the carriers identified in these examples have either implemented CALEA solutions or contracted with a trusted third party to administer its CALEA responsibilities.

U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION, THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT, AUDIT REPORT 06-13, xi. The report further noted, "Three of the case examples described unsuccessful VoIP intercepts . . . In our judgement, these examples are not necessarily indicative of emerging technology that is negatively impacting law enforcement's ability to conduct electronic surveillance." *Id.* at 48-49.

61. The Petition, *supra* note 57, at 5-9.

CALEA compliance for packet-mode technologies.[62] According to the petition, the issue was that "the industry standards-setting organizations did not agree with Law Enforcement's position that industry is required to provide the same level of capability for packet-mode technology as it does for circuit-mode technology."[63] There was, however, ample evidence that the service providers were indeed working with law enforcement to develop VoIP wiretapping standards.[64] The FBI's stance is that compliance to these standards is voluntary and thus not reliable.

Despite the problems with the FBI's interpretation of CALEA, and despite the lack of evidence of actual harm, the FCC supported the FBI's interpretation. In August 2005, the FCC announced that broadband Internet providers of VoIP must comply with CALEA.[65] This was followed by a statement of FCC policy: "To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement,"[66] which was acknowledged to be about making it illegal for Americans to use such VoIP providers as Skype and PGPfone unless the software complied with CALEA.[67]

The FBI's petition produced a strong response from the telecommunications and computer industries and civil liberties groups; many raised the important legal issue that CALEA specifically exempted information services. This issue, while quite important, is not the focus of this article; our attention is on the security consequences of applying

62. *Id.* at 34-40.

63. *Id.* at 34-35.

64. The industry-developed surveillance standards include the Cable VoIP Solution, the Wireline VoIP Solution, the UMTS/GPRS/GSM VoIP Solution. *See* http://www.askcalea.net/standards.html, a website maintained by the FBI.

65. The actual rule appeared in 70 Fed. Reg. 197, 59664 (Oct. 13, 2005).

66. *In re Appropriate Framework for Broadband Access to the Internet over Wireless Facilities,* CC Dkt. No. 02-33 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services,* CC Dkt. No. 01-337 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review —– Review of Computer III and ONA Safeguards and Requirements,* CC Dkt. Nos. 95-20 & 98-10 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities,* CC Dkt. No. 00-185 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities,* CS Dkt. No. 02-52 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf *;* POLICY STATEMENT*,* FCC 05-151 3 (September 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

67. Declan McCullagh, *FBI to get veto power over PC software?*, News.Com (Sept. 27, 2005), http://news.com.com/2061-108043-5884130.html.

CALEA-type laws to VoIP, rather than the specific applicability of CALEA to VoIP.

The FBI's current focus is on packet-based communications technologies, which function rather differently than the circuit-switched telephone system. VoIP consists of routing voice conversations over the Internet or using Internet protocols. Voice is digitized, then broken into packets and sent over the Internet. The wide use to which packet-switched technology is being applied, and the differences between circuit-switched and packet-switched networks, mean that the application of wiretapping to information services is not straightforward. The next section explains how network-switching technology works, laying the groundwork for the later discussion of the dangers posed by applying CALEA to VoIP.

## III. HOW DOES NETWORK-SWITCHING TECHNOLOGY WORK?

Although the public switched telephone network (PSTN) and the Internet are both communications networks, the architecture of the two networks is quite different. That difference has many consequences. A big difference is that the Internet is much simpler to subvert than the telephone network. To comprehend this difference, it is necessary to attain a basic understanding architecture in order to see the security difficulties that arise from applying CALEA to VoIP.

The PSTN is a circuit-switched network. When a call connection is created, the two parties[68] establish a direct path between them. For the duration of the call, only the two parties communicating use this path; it is a temporary, but dedicated, connection.

That picture is a bit of an oversimplification. In digitally-switched networks, it is possible to do "time division multiplexing." The data stream is divided into time slots; the temporary-but-dedicated connection is actually the time slot in the data stream, rather than the entire data stream.[69] That time slot is reserved even when the communicating ends are silent (and, of course, in a conversation typically one party is silent at any given time).

Callers connect through the *local exchange,* which is also known as the *central office.* Connections between the central offices are provided by a *tandem center,* which connects central offices that are not directly connected to each other. There is a hierarchy of such tandem offices, which serve increasingly larger areas.[70]

---

68. For the purposes of this paper, we will limit ourselves to communications between a pair of users, rather than considering multi-party communications.

69. ANDRÉ GIRARD, ROUTING AND DIMENSIONING IN CIRCUIT-SWITCHED NETWORKS 431 (1999).

70. UYLESS BLACK, COMPUTER NETWORKS: PROTOCOLS, NETWORKS, AND

The network routes calls through the cheapest available path. This is typically the shortest path, though it could be the one with the fewest number of switches, the least congestion, etc. Such routing reduces call delay.[71] Years ago, switches were mechanical objects physically connecting the wires that linked the callers. Now, of course, the switches are computers. The job of the computerized switches, however, remains much the same; the computer switches function as did the mechanical switches of old, albeit far more efficiently. In particular, the computer switches do not provide storage; the call comes in and goes out with no information stored at the switch.[72]

By contrast, the Internet is a "packet-switched" network. In such networks, fixed circuits are not dedicated for the duration of a communication. Instead, the data that is transmitted, whether files, email, Instant Messages, voice, is broken into small packets. Each packet travels its own route over the Internet. The entire set of contents is reassembled when it is received at the other end. The technology of packet routing creates some differences with circuit-switched technology.

In particular, the routes packets traverse is dynamically determined through addresses carried in the packets themselves. If a particular communication link is busy, the packet will be routed through a less-congested path. In theory — this occurs much less often in practice — each packet of a communication may travel a different route to its destination.

Another difference from circuit-switched technology occurs at the switches: the dynamic aspect of Internet routing means that it is a "store-and-forward" network; a switch waits to receive the entire packet contents before any of the packet bits are shipped out. Store-and-forward enables transmission in a network where nodes may be temporarily inaccessible. The bits of the packet sit at the switch before they are forwarded on. By contrast, none of the bits sit around at a telephone switch.

Although Voice over IP is a packet-switched technology, it has some different characteristics from other packet-switched applications such as file transfer and email. The most significant of these is that VoIP suffers serious quality-of-service problems if there is more than a 150 millisecond latency in packet delivery.[73] More precisely, VoIP must achieve the 150 millisecond bound in order to successfully emulate

---

INTERFACES 11-12 (1987).

71. *Id.* at 12-13.

72. *Id.* at 166.

73. U.S. DEP'T OF COMM., Special Pub. No. 800-58, D. Richard Kuhn et al., *Security Considerations for Voice over IP Systems: Recommendations of the National Institute of Standards and Technology* 19 (Jan. 2005).

current circuit-switched communications systems. This means that many of the standard security products, including firewalls,[74] network translation routers,[75] and virtual private networks,[76] all of which create latency by interposing additional functionality, are problems for VoIP.[77]

Wiretapping is performed somewhat differently on the two networks. A phone call may theoretically be wiretapped at any point along its path, although the most common place is at the frame — the set of racks at the local telephone exchange that place the incoming lines in numerical order.[78] Prior to the computer era, a tap was a physical object (just as was shown in all the old film noir). Modern switching technology, such as AT&T's ESS series and Northern Telecom's DMS-100, has simplified police wiretapping. Now the tap can be accomplished through the switch's ability to create conference calls. The tap is, after all, a conference call with a silent – and unacknowledged – third party.[79]

Wiretapping VoIP is simultaneously harder and easier than tapping a conventional phone call. On the one hand, because a telephone call always go through a central office, there is a natural place to tap circuit-switched calls. And because a telephone call uses a fixed circuit, a circuit-switched call is simpler to tap than a VoIP call, in which each packet route is dynamically generated. If one knows the IP address of the machine on which the VoIP call is being made —- this is the case for fixed devices (e.g., an office computer) —- then knowing where to place the wiretap on a VoIP call is easy. Otherwise it is not. The IP address, the Internet location of the computer on which the call is being made, may be one address when the user is calling from Starbucks at 3, another address using the free wireless lobby of the Hilton at 4, and still another from the airport lounge at 5. The changing nature of a user's IP addresses results in real complexity in placing a wiretap on the user's VoIP communications.

A variety of Internet security vulnerabilities make VoIP, which uses the packet-switched network, easy to intercept. The possibilities for

74. A firewall is a configuration of machines and software that prevents unauthorized users from accessing a computer network.

75. Network Address Translation boxes, or NATs, are devices, typically routers, that conform to an IETF standard enabling an endpoint to support more IP addresses than appear to the outside network. The NAT performs address translation to convert "public" addresses to "private" ones within the network.

76. Virtual Private Networks, or VPNs, are private networks configured within a public one, e.g., a corporation network running within the public Internet. Cryptography is often used to achieve confidentiality of the communications.

77. *See* Kuhn, *supra* note 73, at 19.

78. PATRICK FITZGERALD & MARK LEOPOLD, STRANGER ON THE LINE: THE SECRET HISTORY OF PHONE TAPPING 61-62 (1987).

79. DIFFIE & LANDAU, *supra* note 19.

interception include packet sniffers,[80] a web server interface for a VoIP switch or voice terminal, ARP cache poisoning[81] or flooding, etc. These possibilities for interception, however, do not necessarily simplify the problem for law enforcement.

The reason that the Internet is less secure than the PSTN is subtle. In essence it is because the Internet offers a much broader range of services. These services are sufficiently flexible that the Internet is able to make use of them in its own management. But the flexibility and dynamism of the Internet comes at a cost, namely the flexibility and dynamism make the Internet a much more difficult system to manage and secure. There are also other security differences between the two types of networks.

There are substantially different expectations regarding reliability of the two networks. Telephone networks are expected to have "five 9s" reliability, meaning that the network is available at least 99.999% of the year (which translates to under six minutes of outage annually). Few Internet-based systems are expected to be similarly reliable. Despite that, over the last two decades, modern societies have come to rely on two network communications systems: the circuit-switched telephony network, and the packet-switched Internet.

Thus, we are left with a set of complicated technological and policy issues. It is clear that for market and national security reasons, VoIP calls must enjoy the same privacy and security that circuit-switched telephony currently does. Yet in VoIP we have a technology that is more difficult to secure than traditional telephony. We also have a law-enforcement agency that would build security vulnerabilities into the communication protocols; these are issues we will explore in the next section.

## IV. TECHNOLOGY RISKS POSED BY THE FBI'S PROPOSAL

Building surveillance technology into Internet communications protocols will create vulnerabilities. Some of the issues raised regarding

80. A packet sniffer is a hardware device or software program that monitors (passively intercepts) packets traversing a network.

81. Each device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The former is "permanent"; it resides on the physical network card inside the device, the latter is "dynamically" assigned, and can change if the device moves networks (or within the network). In order for information to be delivered to a device on the network, there needs to be a way to associate the MAC address with the IP address; this is the Address Resolution Protocol, or ARP. For efficiency's sake, the ARP information is kept in a cache, the ARP cache, so that it does not need to be looked up each time information has to go somewhere. "ARP cache poisoning" occurs when corrupt information is fed to the ARP cache, giving a false IP address to be associated with the MAC address.

the application of CALEA to VoIP are broader than technological security, e.g., the loss of U.S. competitiveness, while others are more narrowly focused. In this section, I discuss the technological problems raised by applying CALEA to VoIP.

### *A. The End-to-End Rule in Internet Architecture*

The fundamental principle used in designing the PSTN was high quality for its most important application: voice transmission. The endpoints — the phone receivers — are dumb. In contrast, in the Internet, the intelligence is at the endpoints. The underlying network system is simple, leaving the endpoints able to deploy complex systems. The thought behind this design principle is that only the architects of the function in question would be in a position to fully understand what the application needed, and thus they should be the ones to provide it.[82]

The architectural idea of intelligence at the endpoints enables the Internet's versatility. Applications can be designed far beyond what the original designers of the Internet had in mind. Innovation has flourished because the simplicity of the Internet means that no one needs to depend on – or wait for – changes in the infrastructure in order to innovate. Thus applications as diverse as Google,[83] eBay,[84] and Skype[85] can be developed without changes to Internet infrastructure. The Internet's design flexibility comes at a price that we do not often think of as a price (we usually find it a benefit): the Internet is hard to control. This does not mean political or border controls (though those are also difficult to implement on the Internet), but design control. The flexibility afforded by the Internet to new applications means that there are few barriers to entry. The Internet boom of the late 1990s, seen by many as only the first step of the Internet revolution, was greatly facilitated by the low barrier to entry for new applications.

Marjory Blumenthal, Executive Director of the Computer Science and Telecommunications Board of the National Research Council from 1987-2003, and David Clark, one of the early Internet architects, and Chief Protocol Architect from 1981-1989, observed,

> When end points want to communicate, but some third party demands to interpose itself into the path without their agreement,

82. J.H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS, 277, 278 (1984) ("The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system").

83. Google is currently the world's most popular search engine. *See* http://www.google.com.

84. Ebay is the originator of online auctions. *See* http://www.ebay.com.

85. Skype is a free Internet telephony service. *See* http:///www.skype.com.

> the end to end arguments do not provide an obvious framework to reason about this situation. We must abandon the end to end arguments, reject the demand of a third party because it does not 'fit' our technical design principles, or find another design approach that preserves the power of the end to end arguments as much as possible.[86]

Wiretapping is such an interposition. Building wiretapping capabilities into the Internet anywhere but the endpoints would require a fundamental change to Internet architecture. Thus applying CALEA to VoIP breaks the Internet's traditional end-to-end model.

Indeed, no longer would a small group of innovators be able to have an idea, develop it, and go to market; instead, early on, they would need to consult with the FBI. They would need lawyers and lobbyists — and time.[87] Such a process is hardly a useful way to encourage Internet innovation. The U.S. holds no lock on the ability to innovate. In the last decade, the Earth has become "flat"; research and development is burgeoning in China, India, and elsewhere.[88] Globalization, computing power, the Internet, and broadband have combined to enable business and research to flourish across the globe.

In threatening innovation, the FBI proposal not only poses problems for U.S. industry, but also for national security. Scientific and industrial strength were critical components of U.S. strength during both world wars and remain so today. A program that threatens domestic Internet innovation ultimately threatens national security.

### *B. The Internet and Critical Infrastructure*

Complicating the national security issue, much of society's infrastructure now runs using Internet protocols. The Internet is an efficient and inexpensive communications medium, and the last decade has seen a massive shift to the Internet or to private networks using Internet protocols as the communications medium of choice. This shift was the result of millions of small decisions, and these were made even though the Internet protocols were insecure. There is no turning back.

This reliance on the Internet, and on Internet protocols, in turn raises concerns about the security of packet-switched networks, an issue explored by numerous recent government studies.[89] The control

---

86. Marjory Blumenthal & David Clark, *Rethinking the design of the Internet: The End to End Arguments vs the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70, 73-74 (2001).

87. The recent FCC decision that VoIP must support E911 access presents many of the same threats to innovation.

88. *See generally* THOMAS L. FRIEDMAN, THE WORLD IS FLAT (2005).

89. *See e.g.*, JAMES ELLIS ET AL., PRESIDENT'S COMMISSION ON CRITICAL

infrastructure for various sectors, including electricity, water, and oil pipelines, uses a combination of private lines, leased lines, radio transmissions, and the Internet for communications. In recent years, in some cases the process control networks have been integrated with the business networks in order optimize dynamic pricing — e.g., raising and lowering the rates for electricity as capacity allows. But the business networks are, of course, connected to the Internet and thus that linkage leads to potential vulnerabilities. This threat is not merely theoretical.

Breaches have included a hacking incident into a telephone "loop carrier" switching system that disabled the Worcestor Airport's tower communications, shutting down the airport for six hours.[90] A similar attack on a sewage treatment plant in Maroochy Shire, Australia resulted in a release of thousands of gallons of untreated sewage into the local area.[91] The Slammer worm infected the Davis-Besse nuclear power plant, disabling a safety monitoring system (because the plant was shut off at the time, there was no immediate danger). The worm reached the plant through a machine on an unsecured network of a private contractor, thus bypassing the plant's firewall.[92]

Protecting critical infrastructure has taken on a new urgency. It is not just terrorists who are likely to target the networks supporting critical infrastructure; the Chinese government, for example, has "invested significantly in cyberwarfare training and technology,"[93] and Japan has already suffered a number of attacks originating in China and South Korea.[94] Cyberattacks on networks, especially in a vulnerable nation such as Taiwan, can have as destabilizing an effect as attacks on physical infrastructure.

Critical infrastructure information is not the only kind of private information that merits protection. Many types of corporate information, including those not directly dealing with critical

---

INFRASTRUCTURE, REPORT OF THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (1997); PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BD., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (Feb. 2003); UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO THE COMMITTEE ON ENERGY AND COMMERCE, HOUSE OF REPRESENTATIVES, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES FOR SELECTED AGENCIES AND SECTORS (2003).

90. Paul Festa, *DOJ Charges Youth in Hack Attacks*, News.Com, http: //news.com.com/2100-1023_3-209260.html (March 18, 1998).

91. Dana Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat,* CRS REPORT FOR CONGRESS 7 (2003).

92. Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant*, The Register, http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/ (Aug. 20, 2003).

93. Robert Kaplan, *How We Would Fight China*, ATLANTIC MONTHLY, Jun. 2005, at 54, 55.

94. Anthony Faiola, *Anti-Japanese Hostilities Move to the Internet*, WASH. POST, May 10, 2005 at A12.

infrastructure information, need protection as well. For decades, U.S. companies have suffered from attacks on their unsecured communications systems. An incident from the 1970s illustrates the dangers that can result to the nation because of unprotected communications of private companies.

The Soviets had installed a major electronic eavesdropping center in the top floors of a house in Glen Cove, New York. The house was adjacent to Long Island Sound's "microwave alley," where much of the East Coast's communications traveled.[95] The Soviet equipment was capable of picking up conversations from a distance of one hundred miles. IBM was alerted that its corporate communications were not secure.[96] Nor were the communications of other companies. "[T]he Soviets could monitor all the telephone calls to and from the Department of Agriculture, and they ended up knowing more . . . than we did," a CIA veteran told the press.[97] That knowledge proved useful to the Soviets, who ended up buying up U.S. wheat at a favorable price. Meanwhile the U.S. ended up with a wheat shortage. Such incidents are not isolated to the 1970s. As recently as the 1990s, at least one U.S. manufacturer was warned by government officials that its microwave communications were vulnerable to eavesdropping.[98]

### *C. Network Architecture and Wiretapping*

The layered[99] approach of Internet architecture does not preclude wiretapping. There is nothing inherent in the design of a communications network that precludes security or wiretapping, and indeed there are defense communications networks that simultaneously provide security and wiretapping capability. The Internet was originally designed as a resource-sharing network; neither security nor wiretapping were considerations in its initial design. While it is technically feasible to build an Internet that has intercept facilities with adequate security, it is unlikely to be politically or socially possible to do so now.[100]

---

95. William Broad, *Evading the Soviet Ear at Glen Cove*, 217 SCIENCE 910, 911 (1982).

96. KENNETH DAM ET AL., CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 68 (1996).

97. Broad, *supra* note 95, at at 910.

98. DAM ET AL., *supra* note 96, at 68.

99. The Internet architecture is designed as a layered model, in which each layer uses the functions of the layer below. The seven layers are: physical, data link, network, transport, session, presentation, and application. The lower links are typically implemented in hardware, the upper ones, in software.

100. Fifteen years ago a transition to such a network might have been possible. If the U.S. government had sought, through a combination of R&D funding and other financial incentives to the ISPs, to create a secure Internet that enabled surveillance, it is possible that such a system could have been built. After all, at that time, the Internet was a U.S.

If laws or regulations were to require building access into Internet communications for U.S. law enforcement or national security, it is unlikely that such a protocol design could be accomplished securely. Building such requirements into managed networks (networks with central control) presents no serious technical difficulty. Building them into the peer-to-peer network that constitutes the Internet, however, does.

The Internet Engineering Task Force (IETF) creates the protocols that enable the Internet to work. These protocols must be carefully specified so that computers on the Internet can interoperate. In 2000 the IETF Network Working Group studied implanting wiretap requirements into Internet protocols. Their conclusion was that it could not be done securely.[101]

Such a conclusion stems from fundamental engineering principles. Complexity is the bane of security; additional program functionality increases the likelihood of a security breach.

### *D. The Threats are Real*

By deliberately leaking information to a third party, wiretapping is an architected security breach. A recent hacking incident at Cisco illustrates the dangers of building wiretapping capabilities into the Internet.

Despite the IETF's reluctance to write wiretapping into network protocols, Cisco forged ahead, developing a proprietary architecture for VoIP interception at the router level. The interception would be performed by ISPs.[102] For this technology to function appropriately — and *not* deliver packets to unauthorized parties — the ISP network itself would need to be secure, a challenge for ISPs. Given that, it is ironic that Cisco was unsuccessful in protecting itself from a year-long Internet attack by a small group (possibly only a single individual) that succeeded in penetrating the router company and accessing protected information.[103] Despite notice of the repeated attacks, the company was

---

phenomenon and international cooperation was not required. That is not the case now. The Clipper lesson from a decade ago speaks loudly here. Foreign governments were simply not interested in a program in which the U.S. government held the encryption keys and so the U.S. found it impossible to arrange multi-lateral key-sharing agreements. There is no reason to suppose that such arrangements could be made now to enable a secure, surveillance-capable Internet.

101. Internet Architecture Bd. & Internet Eng'g Steering Group, IETF Policy on Wiretapping, RFC 2804 (2000), *available at* http://www.faqs.org/rfcs/rfc2804.html [hereinafter IETF POLICY ON WIRETAPPING].

102. FRED BAKER ET. AL., CISCO SYSTEMS, CISCO ARCHITECTURE FOR LAWFUL INTERCEPT IN IP NETWORKS, RFC 3924 (2004), *available at* http://www.faqs.org/rfcs/rfc3924.html.

103. John Markoff & Lowell Bergman, *Internet Attack Is Called Broad and Long*

nonetheless unable to prevent theft of proprietary software.

Building CALEA into VoIP would require security maintenance by the ISPs. Would ISPs be able to keep their "architected security breach" — the shipping of data to an authorized third party — fully secure? The ISPs, especially many of the smaller ones, are likely to be more vulnerable than Cisco.

Modern design paradigms make the problem worse. In the 1950s, if the NSA wanted copies of telegrams from the telecommunications companies, tapes with the telegrams were picked up by NSA courier.[104] The current model for tapping VoIP calls requires sending the bits via the Internet. Thus wiretapping is an architected security breach with the data automatically shipped remotely.[105] Enabling the remote delivery of data to a third party provides another potential for a security breach. In particular, the dangers posed by insider attacks continue to be much greater than the dangers posed by hackers. A rogue insider with the capability to conduct remote data delivery increases the likelihood that unauthorized surveillance will go undiscovered.

This is not a speculative threat. Recently, around one hundred mobile phones of members of the Greek government— including the prime minister—were illegally tapped for over a year.[106] This incident involved exactly the same architected security breach that wiretapping VoIP calls would require. Ericsson, a telecommunications supplier, had provided software to Vodafone that included "locked" eavesdropping capabilities. Someone at Vodafone subverted the system, activated the eavesdropping, and had the tapped communications delivered to a set of fourteen mobile phones. These events illustrate the potential for a rogue insider using the remote-management capabilities provided by a legally authorized eavesdropping system.

### *E. Enabling Surveillance by the Bad Guys*

A technology designed to simplify Internet wiretapping by U.S. intelligence presents a fat target for foreign intelligence agencies. Breaking into this one service could yield broad access to Internet communications without the expense of building an extensive intercept

---

*Lasting*, N.Y. TIMES, May 10, 2005, at A1.

104. This was what was done during the "Shamrock" program, where tapes of all international telegrams from RCA Global, ITT World Communications, and Western Union International were shipped daily to the NSA.

105. This was the case, for example, with the FBI system for tapping email, Carnivore (now renamed DCS-1000).

106. *Spy Software Used in Mobile Eavesdropping*, KATHIMERINI ENGLISH EDITION, Feb. 3, 2006, *available at* http://www.ekathimerini.com/4dcgi/news/content.asp?aid=65958; Fotini Kalliri, *Wiretaps Kept Quiet for Eleven Months*, KATHIMERINI ENGLISH EDITION, Feb. 13, 2006, *available at* http://www.ekathimerini.com/4dcgi/news/content.asp?aid=66340.

network of their own.[107] Remote monitoring capabilities would mean that system vulnerabilities are thus as likely to be global as local. Were Internet wiretapping technology to be penetrated and exploited by foreign intelligence services, massive surveillance of U.S. "persons" (citizens and corporations) might follow.

There is another major infrastructure change that would further enable penetration and exploitation, namely the development over the last decade of very powerful search engines. Information that was public but was largely inaccessible, enabling security through obscurity[108] as it were, has now become trivial to discover and access. Internet wiretapping technology used in combination with inexpensive automated search technology could lead to an unprecedented compromise of U.S. security and privacy.

This problem is further aggravated by the direction of the Internet's development. Building surveillance capabilities into the Internet infrastructure, and not into the application endpoints, would expose to eavesdropping not only current applications but also future ones. Currently, there are millions of devices connected to the Internet, but we are rapidly moving to a situation of billions of resource-limited small devices such as radio-frequency identification (RFID) tags and sensors that will communicate via the Internet.

RFID tags are small devices with a computer chip and an antenna; they can receive and respond to radio-frequency queries from a transmitter. They are often the size of a barcode – a technology they will eventually replace – and they provide some of the same functionality, only more so. Cheaper RFID tags are passive, and only respond to a query, while more expensive tags have their own power sources that allow them to write on their tags as well as giving them longer ranges of broadcast. Tags respond to a signal from the reader and then transmit information, enabling functions like rapid authentication for entrance to secure facilities, product identification that enables tracking of goods, and the like. There is much more data on an RFID tag than a barcode, so that the RFID tag is able to identify not only the type of item – a Prada handbag – but the individual item itself – a Prada handbag sold at the Manhattan Saks Fifth Avenue on July 14, 2005. RFID tags will soon

107. Susan Landau, *Security, Wiretapping, and the Internet*, 3 IEEE SECURITY & PRIVACY 31, (Nov./Dec. 2005), *available at* http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/sp/&toc=comp/mags/sp/2005/06/j6toc.xml&DOI=10.1109/MSP.2005.158.

108. The term "security through obscurity" is usually used to describe hiding security mechanisms in order to make them difficult to foil. Security through obscurity is viewed as a poor way of doing security, since what the methodology gains by secrecy is typically much less than what it loses through the lack of a public review. In the case I am describing here, the obscurity was accidental, an artifact of the previous difficulty of search.

be everywhere for use in inventory control, whether it be clothing or razor blades, for livestock tracking systems, for airline baggage handling, for logistics support for the Defense Department.

Sensor networks are networks that hook together small, inexpensive devices that measure such physical attributes as temperature, sound, and vibration. The sensors themselves have limited computing power and a limited energy supply. Sensors will be used in a myriad of remote monitoring scenarios, such as tracking environmental conditions or monitoring the state of elderly patients.[109] The devices themselves have limited memory, the networks have limited bandwidth, and there is also a lack of a priori knowledge of post-deployment configuration,[110] meaning the sensors do not know what the topology of the network is.

Neither RFID tags, which have been employed in the highway toll booth system for years, nor sensor networks, which were used during the Cold War to track the movement of Soviet submarines,[111] are new. What is new is the dropping cost of these technologies, which is enabling them to have a much wider range of uses. We are moving to a world of billions and billions of devices[112] that will be connected to the Internet.

Much of the data from RFID and sensor networks will remain in local area networks and not travel the Internet, but some types of data gathered will be aggregated in a central database. More to the point, the cheapness and ubiquity of the RFID and sensor technology means that even if a small percentage of these networks communicate via the Internet, this will provide a significant new and unprotected data source on the Internet. Both RFID tags and sensors are sufficiently small and low-powered that providing security is difficult. (Adequate security is, of course, dependent on context. The security needed to protect the data of an RFID tag on a razor on a Wal-Mart shelf is very different from the security needed to protect the data of an RFID tag on a diplomatic passport.)

### *F. We've Had This Battle Before*

In 1996, the National Research Council released the report

109. For example, pulse-oximetry sensors would measure and report heart rate, rate of blood flow, and blood oxygen saturation.

110. Haowen Chan & Adrian Perrig, *Security and Privacy in Sensor Networks*, 36 COMPUTER 103, 103-05 (Oct. 2003), *available at* http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/co/&toc=comp/mags/co/2003/10/rxtoc.xml&DOI=10.1109/MC.2003.1236475.

111. The Sound Surveillance System (SOSUS) did this through hydrophones – long acoustic sensors – arrayed on the ocean floor.

112. The increase will also be fueled by portable personal communicating devices, e.g., cell phones and PDAs.

*Cryptography's Role in Securing the Information Society*.[113] The report's authors, among them a former deputy secretary of state, a former U.S. Attorney General, a former deputy director of the National Security Agency, and a former president of the Institute for Defense Analysis, concluded that, "[o]n balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[114] Over the last several years, the government sought improvements in civilian communications infrastructure security, even though some of those improvements were likely to impede law enforcement investigations. The shift was clearly supported by the intelligence agencies, which found that the societal gains from increased information security outweighed the disadvantages to national security and law enforcement investigations. In addition, the military's move to save money by purchasing commercial off-the-shelf equipment meant that increases in the security of commercial equipment directly benefit defense agencies, enabling them to obtain the security they need without the necessity of producing custom products.[115]

The battle over applying CALEA to VoIP is in many ways reminiscent of the "Crypto Wars" of the 1990s. During that period, the FBI sought, through CALEA and the ill-fated Clipper key-escrow system, to hold on to its 1960s wiretapping capabilities in the face of advanced digital-switched telephony and other forms of digital communications. The Clipper program, announced in 1993, was a federal standard for protecting communications through an 80-bit cryptosystem and keys escrowed with agencies of the federal government. There were objections from industry and from civil liberties groups. In any case, international acceptance of the program, crucial for its success, never developed. As a result, the project was a dismal failure and few systems using it were ever built.[116]

In 2000, when U.S. national security agencies decided that the nation was better served through the deployment of strong cryptography,[117] support for the FBI position eroded and U.S. policy changed.[118] In part, the national security position changed because the

113. *See* Dam et al., *supra* note 96.

114. *Id.* at 6.

115. *See, e.g.*, Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th Century and the 21st*, *in* SUN MICROSYS LABS: THE FIRST TEN YEARS 1991-2001, SUN LABS PERSPECTIVES ESSAY SERIES 410-15 (Jeanie Treichel & Mary Holzer eds., 2001), *available at* http://research.sun.com/techrep/Perspectives/PS-01-5.pdf.

116. *See id.* at 210-15.

117. This was not ever explicitly stated by the U.S. government, but the change to a more liberalized set of cryptographic export control rules would not have occurred without the support of the national security agencies.

118. The Department of Commerce, Bureau of Export Administration issued 15 C.F.R. Parts 734, 740, 742, 770, 772, and 742, Docket No. RIN: 0694-AC11, effective January 14, 2000. These would not have been issued without the strong support of the national-security

NSA and other agencies realized that the use of strong cryptography throughout the infrastructure – the protection of civilian information – was in many ways far more important than enabling law enforcement investigative techniques. In recent years, the government has encouraged a number of cryptographic efforts, including the development of the 128-bit Advanced Encryption Standard and the Elliptic Curve Cryptosystems.[119] Then, as now in the VoIP debate, the FBI pushed for the extension of wiretapping capabilities even though it could pose serious dangers to the protection of civilian information, including critical infrastructure.

A decade ago, Congress faced the dual issues of surveillance and communication security when it confronted CALEA and Clipper. Congress passed the wiretapping bill, but held a more jaundiced view of the key escrow program. A number of Senators and Representatives took positions against the Clipper chip.[120] In CALEA, Congress also explicitly excluded information services from the law's requirements. Congress' view was that wiretapping – and CALEA – makes sense for law enforcement in the PSTN environment, but issues of information security take precedence in the Internet environment.

At present, we are struggling to achieve adequate security in the Internet without intentional security compromises in its design. Although it may one day be possible to incorporate surveillance into packet-switched networks with sufficient security, it is hard to see how this could be less difficult than the unfinished task of developing scalable and economical secure networks. At the very least, built-in wiretapping would require secure communications of its own in order to carry the intercepted information to the customers for which it was being collected.

These changes do not mean that Internet communications cannot be wiretapped. The insecurity of the Internet is well known. Currently, few communications are routinely protected (e.g., encrypted end to end). As the IETF Network Working Group observed, "the use of existing network features, if deployed intelligently, provides extensive opportunities for wiretapping."[121] But exploiting current insecurities and

---

agencies.

119. *See* NIST Computer Sec. Div. Computer Sec. Res. Ctr. Focus Areas, http://csrc.nist.gov/focus_areas.html#csa.

120. In 1996 Senator Patrick Leahy introduced the Encrypted Communications Privacy Act of 1996 (S. 1587, 104th Cong. (1996)), which affirmed the right to use any form of encryption domestically. Meanwhile Senator Conrad Burns proposed a bill prohibiting mandatory key escrow and enshrining the freedom to sell and use any type of encryption domestically, and liberalized export rules. In the House, Representative Bob Goodlatte proposed a similar bill (H.R. 695, 105th Cong. (1997)). *See also* Diffie & Landau, *supra* note 115, at 222-23.

121. IETF POLICY ON WIRETAPPING, *supra* note 101.

actually building insecurities into Internet protocols have significantly different effects on the security of society's communications. I am arguing against the latter; I take no issue with the former.

## V. SECURITY FROM A BROADER VIEWPOINT

The FBI is a law enforcement agency and it does what law enforcement agencies do: investigate crimes, arrest the perpetrators, and provide evidence for conviction. As a law enforcement agency, the FBI is committed to tools that can provide a "chain of evidence." This approach has proved successful in fighting organized crimes, drug dealers, and white collar crime. Law enforcement's view of what works in terrorist cases can be summed up by the 1991 statement of then FBI Director William Sessions: "[i]f a terrorist attack does occur, it is our view that a swift and effective investigation culminated by arrest, conviction and incarceration is a powerful deterrent to future acts of terrorism."[122] The evidence, including terrorists who were willing to fly airplanes into buildings in order to achieve their goals, would argue otherwise.

In the fight against violent fundamentalists, the FBI approach and tools are often inappropriate.[123] For example, given that the violent Islamic fundamentalist movement, has a potential base of millions, U.S. strategy must take into account that the war must be fought politically and economically, as well as militarily.

In earlier parts of this article, I argued that CALEA applied to VoIP is a poor security solution from a technological vantage point. In this section, I will show that ubiquitous surveillance technology proposed by the FBI is also a poor solution from a policy standpoint. I begin with putting various myths to rest.

We begin with the fact that September 11th was not the first instance of domestic terrorism in the United States. American history is replete with examples of homegrown terrorism, from Presidential assassinations, to racial terrorism exemplified by the Ku Klux Klan, to right-wing militias such as Posse Comitatus and the Order.

Nor is al Qaeda the first imported version of terrorism. Before the U.S. entry into the First World War, in an undeclared war, German saboteurs sought to cripple U.S. war production efforts. Though fewer

---

122. *FBI Programs: Hearing Before the Subcomm. on Civil and Constitutional Rights, Comm. on the Judiciary*, 102d Cong. 269-70 (1991) (statement of William Sessions, Director, FBI).

123. Violent Islamic fundamentalists are of greatest concern right now, but they are not the only religious zealots who have turned to violence; other examples include the rise of Hindu fundamentalism in India and the anti-abortion zealots who have turned to violence in the U.S.

lives were lost in terms of physical damage, the destruction was on a significantly greater scale than the destruction of the World Trade Center. The damage included the total destruction of a major munitions depot, blowing up over two million pounds of explosives, and many other acts of terrorism, including bombings of ships and chemical plants.[124]

Recent domestically-generated terrorism has included the Oklahoma City bombing and attacks on abortion clinics. These attacks, however, were neither on the scope nor scale of the attacks of September 11th, whose aftereffects include a radical reworking of U.S. domestic and foreign policy.[125] The National Commission on Terrorist Attacks upon the United States,[126] hereinafter referred to as the "9/11 Commission Report," observed that, "[t]he [terrorism] fostered by bin Laden and al Qaeda were on a scale approaching acts of war . . ."[127] Despite this, strategies to prevent terrorist attacks conform more closely to law enforcement practices than national security goals. There are a number of reasons for this.

One is psychological. There is simple comfort in viewing Islamic terrorism as criminal acts; "[if] bin Laden is a criminal whose activities are fueled by money – not a devout Muslim soldier fueled by faith – . . . Americans know how to beat well-heeled gangsters."[128] From the sheriffs in the Wild West, to the FBI ridding Chicago of its gangsters in the 1930s, the U.S. has a powerful mythology of the good guys always getting their man. The nation does not always win wars, but in U.S. lore, the sheriff walking down Main Street and the G-men in the dark alleyway always prevail.

A second powerful reason for the law enforcement approach is some

124. Black Tom Island, a munitions storage depot in New York Harbor, was blown up on July 30, 1916. The explosions destroyed windows in nearby Jersey City, as well as in Manhattan and Brooklyn; blasts were heard in Philadelphia (a hundred miles away). A total of over two million pounds of explosives were destroyed. Six-and-a-half months later, the huge shell-assembling plant of the Canadian Car and Foundry Company in Kingsland, New Jersey, which was building weaponry for Russia, was completely destroyed in a deliberately-set fire. The cost: seventeen million dollars. HENRY LANDAU, THE ENEMY WITHIN: THE INSIDE STORY OF GERMAN SABOTAGE IN AMERICA 77-91 (1937). In all, including fires and explosions in factories and in ships, German saboteurs caused over one hundred and fifty million dollars in damage to essential war goods. *Id.*

125. The controversial USA Patriot Act, as well as various regulations regarding air transportation initiated by the Transportation Security Administration, are one set of examples; another is the creation of the Department of Homeland Security; a third, and perhaps the most significant, are the two foreign wars fought since September 11th, in Afghanistan and in Iraq.

126. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S. (Comm. Print 2004).

127. *Id.* at 348.

128. MICHAEL SCHEUER (PUBLISHED AS ANONYMOUS), IMPERIAL HUBRIS: WHY THE WEST IS LOSING THE WAR ON TERROR 348 (2004).

early successes in the "war" on terror. The FBI's investigations of the PanAm plane crash over Lockerbie, Scotland and the first World Trade Center bombing led the public and policymakers to believe that the tools of law enforcement were the appropriate ones with which to combat terrorism.[129] These "missions accomplished" led to an aura of invincibility around law enforcement's capability to conduct the war on terror, an invincibility that continues to permeate the current discussions (which continue to center on there being no, as opposed to few, acts of terrorism occurring in the United States).

What drives law enforcement efforts is conviction in a court of law, but this is a misguided viewpoint. Anti-terrorism efforts could suffer under this type of mindset, because, as former U.S. Deputy Attorney General Philip Heymann has observed, in many cases law enforcement is not a deterrent to terrorists.[130] Violent Islamic fundamentalists often view a jail sentence as a form of martyrdom. Jail also provides an excellent opportunity for recruiting – sometimes amongst the nationals in the country in which the terrorism is to take place.

With its appropriate emphasis on proof, law enforcement investigations seek a level of evidence that will convict. This is not always an appropriate measure in a war against terrorists. As a CIA agent describes the situation,

> "Americans . . .ought also pray that Washington puts away the badge and warrant, and . . .U.S. and Western analytic corps and militaries . . .pull their weight against Al Qaeda by deciding this is a military, not a criminal foe . . .Al Qaeda can never be beaten while the U.S. attack is conceived and executed as an international version of the saga of the American West, where U.S. intelligence officers andsoldiers are sent out, like the storied Texas Rangers, and expected to always get their man."[131]

In spite of Constitutional and jurisprudential requirements of high levels of proof, such a law enforcement approach to terrorism has already incurred significant costs.[132] In contrast, the national security approach to cybersecurity is one of prevention. Currently, one area of national

129. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 72.

130. PHILIP HEYMANN, TERRORISM AND AMERICA: A COMMONSENSE STRATEGY FOR A DEMOCRATIC SOCIETY 79 (MIT Press 1998).

131. *Id.* at 69.

132. During the Clinton administration, for example, law enforcement impeded U.S. government attempts to capture Osama bin Laden. Although this was an accident of the approach, rather than a deliberate impedance, the effect was real. *See* STEPHEN COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN, AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001 425-26, 495 (2004).

concern is the protection of critical infrastructure, much of which uses the poorly-secured Internet for communication; these include the electric power grid, the financial industry, transportation, telecommunications, and the health-care industry. In recent years, critical infrastructure protection has been the subject of a number of Presidential initiatives and is a major focus of the Department of Homeland Security.[133]

The better approach is a blend of the law enforcement and national security strategies. National security on its own can no more solve the terrorist problem than law enforcement can; what we must do is use each approach as it is appropriate to the situation. The desire to knock down the door, arrest the suspect, and go on to the next case should not take precedence over preemptive and proactive security measures.

The struggle against violent Islamic fundamentalists will take place abroad, but as the events of the last decade make clear, attacks will also take place at home. Open communication with immigrant communities is critical for investigation and prevention of terrorism. A surveillance society is likely to alienate these communities. It is crucial to remember that there are two objectives: to save the lives of our citizens and not to lose independence and stability as a nation.[134] This war against violent religious fundamentalists will not be won without the cooperation of domestic immigrant communities.[135] The vast majority of members of these communities are law-abiding U.S. citizens, but as Heymann observes, "[i]n terms of national well-being, the gravest national dangers from a terrorist act (short of an immense escalation of terrorist tactics), are that the interplay of terrorism, public reaction, and governmental response may sharply separate one significant group from the rest of society."[136] In such situations, Heymann notes, "the terrorists will find it far easier to secure communication channels, [etc.]."[137]

As Gilles Kepel observed, "[t]he most important battle in the war for Muslim minds during the next decade will be fought not in Palestine or Iraq but in these communities [of second-generation Muslims] on the outskirts of London, Paris, and other European cities."[138] So far, the United States has been spared home-grown terrorism from violent Islamic fundamentalists; Britain has not. It is instructive to briefly

133. These include the White House. NATIONAL INFORMATION SYSTEMS PROTECTION PLAN, VERSION 1.0 (January 7, 2000); REPORT OF THE PRESIDENT OF THE UNITED STATES ON THE STATUS OF FEDERAL CRITICAL INFRASTRUCTURE PROTECTION ACTIVITIES (January 2001); NATIONAL STRATEGY TO SECURE CYBERSPACE (September 17, 2002).

134. Heymann, *supra* note 130, at xi.

135. *Id.* at 101-02.

136. *Id.* at 2.

137. *Id.* at 13.

138. GILLES KEPEL, THE WAR FOR MUSLIM MINDS 8 (2004).

consider the difference between the Muslim communities in the two nations.

In Britain, South Asian immigrants are three times as likely to be unemployed as white Britons; indeed, forty percent of Pakistani women in Britain are unemployed, as are twenty-eight percent of Pakistani men.[139] But in the United States, the incomes of people of Pakistani origin are close to the median in New York and slightly exceed the median in New Jersey.[140] Britain was a non-immigrant society until after the Second World War. In the United States, by contrast, the South Asian population is following in the footsteps of the many immigrant groups that preceded them, moving up the socio-economic ladder generation by generation. In Britain, the South Asian population is isolated from British society; in the U.S., it is far more integrated. Kepel observes that "it is imperative to work towards full democratic participation for young people of Muslim background."[141]

However, that democratic participation is threatened by domestic intelligence-gathering practices. The warrantless foreign-intelligence wiretaps conducted by the NSA raised fears in the Arab-American and Muslim-American communities. Mountzer Sleiman, a journalist at Al Mustaqbal Alarabi ("The Arab Future"), noted that bin Laden had not been able to recruit Arab or Muslim Americans, but said that, "[the community] feel[s] they are being profiled, under threat, under constant harassment." Sleiman wanted to know if it was "open season on the Arab American and Muslim American in the United States."[142] Such fears in the Arab-American and Muslim-American communities should worry law enforcement. Terrorists seek to split society and then use the split toward their own ends.

The United States is a diverse, multicultural society, woven from many strands. What has held this complex society together is respect for the rights of others, notwithstanding such events as the lynching and state-government-authorized violence against black citizens in the South and the shameful internment of Japanese-Americans during the Second World War. Although early U.S. government responses to the September 11th attacks did not characterize the attacks as a Muslim problem, later government actions have forged a different perception. According to Professor Peter Skerry of Boston College, "events since 9/11 — special registration programs, the Patriot Act, and the war in

139. Nina Bernstein, *In American Mill Towns, No Mirror Image of the Muslims in Leeds*, N.Y. TIMES, July 21, 2005, at A1.

140. *Id.*

141. KEPEL, *supra* note 138, at 295.

142. Questions and comments following remarks by General Michael Hayden, former NSA director, at the National Press Club, Washington, D.C. (Jan. 23, 2006).

Iraq — almost require even secular families in this second generation [of South Asian immigrants] to construct an American identity as Muslims."[143] This is potentially dangerous and without doubt complicates terrorist investigations.

Investigating terrorism cases often means conducting an investigation where the first serious criminal activity – doctored passports and lapsed visas do not count – is often the *only* criminal activity. How do investigators find these people? One way is, of course, the age-old method of following connections. The connections between Khallad Sheik Mohammed, a senior bin Laden security official, and "someone named Midhdar" brought Nawaf al Hazmi and Khalid al Midhdar, two of the September 11th hijackers, to the CIA's attention prior to the September 11th attacks. But another avenue is connections with the community. To be successful, investigators must rely on the good will of the people. As experience in Israel and Northern Ireland shows, harsh investigative techniques – massive searches and surveillance, abuses of prisoners under detention, ill-treatment in jail – often backfire.[144] In Northern Ireland, for example, many believe that the advantages gained through this policing were "offset by the effect of stimulating IRA recruitment."[145]

Sleeper cells pose a particularly serious threat to Western societies, and their investigation requires painstaking work in a community largely composed of law abiding citizens. The need for community cooperation increases many times over when the problem is sleeper cells. Surveillance techniques reminiscent of the repressive regimes that many in the Muslim community fled when they came to the U.S. are likely to alienate the very people who can most aid domestic law enforcement investigations.[146] Building eavesdropping capabilities into the Internet, which undermines such fundamental American values as privacy and freedom of association,[147] will not engender trust in Muslim communities.

In conducting a war against violent Islamic fundamentalists, we must consider what aspects of this war can be won, and what can only be won at too high a cost. Security solutions that also have high adverse social impacts may return much less than they cost in terms of societal cohesiveness and community cooperation. Applying CALEA to VoIP is one such instance.

---

143. Bernstein, *supra* note 139.

144. HEYMANN, *supra* note 130, at 132, 141-42.

145. *Id.* at 126.

146. Europe, particularly Germany and France, have significantly larger Muslim communities than does the United States. In order for these nations to successfully investigate violent fundamentalists, police will need the cooperation of the local communities.

147. *See, e.g.*, NAACP v. Alabama*,* 357 U.S. 449 (1958).

Thinking clearly about which acts can be prevented and which cannot is crucial. Timothy McVeigh's attack on the federal office building in Oklahoma City was the work of a very small group of people. The al Qaeda attacks of September 11th, on the other hand, involved the coordination of a much larger group. Unless we move to a surveillance society on the scale of the former East Germany, a move that runs counter to most of what we hold dear about this country, we will never be able to fully protect against attacks by a "lone" warrior like McVeigh We need to factor such common sense into our thinking about security.[148] Thus, while one can expect surveillance tools to help prevent activities on the scale of September 11th, this is less true for activities carried out by a small group. Depending on the size of the group involved in the London transport bombings, for example, such acts might not be discernable without a level of surveillance intolerable in a free society.

Laws authorizing law enforcement wiretapping were originally passed because of the threat of organized crime.[149] Organized crime works through a small cadre of tightly-linked workers, often family members. This makes the organization difficult to penetrate and complicates investigations. Since radical Islamic fundamentalist groups appear to pose similar investigative difficulties, wiretapping is a particularly tempting tool. But there are also serious differences between investigating organized crime and violent religious fundamentalists, differences that change the value of wiretapping in investigations.

Law enforcement has a far greater deterrent effect on domestic organized crime groups than on those espousing violence as a way to achieve a fundamentalist society. Organized crime does not seek to destroy modern society; terrorists do. A severe disruption of Western democracies would be a major victory for the violent Islamic fundamentalists. And, as discussed earlier, imprisonment is not the same deterrent for violent Islamic fundamentalists for as it is for organized crime figures.

The fact is that wiretapping is unlikely to provide much benefit in tracking terrorists. Al Qaeda is well aware of the eavesdropping and targeting capabilities of the U.S. military and has learned the dangers of communicating electronically. Bin Laden, for example, does not use the

148. HEYMANN, *supra* note 130, at xxi-xxiii.

149. Title III was passed in response to the President's Commission on Law Enforcement and the Administration of Justice, and the original set of crimes that could be investigated using wiretaps were serious crimes that were part of the repertoire of organized crime, e.g., racketeering or interstate transport of stolen goods. The Senate Judiciary Committee Report on Title III said that "each offense was chosen because it was intrinsically serious or because it is characteristic of the operations of organized crime," HOUSE REPORT 90-1097 at 97 (1968).

telephone but instead relies on hand-written messages delivered by trusted couriers. Many terrorist communications are already sufficiently brief and difficult to decipher, not because of digital encryption, but because the communications are written in a code known to the insiders but not to the surveillers.[150]

Thus, in fact, content may not be necessary. Investigators have been quite successful in tracking terrorists without being able to hear the contents of their messages. In a 2002 case, investigators tracked al Qaeda members through terrorists' use of prepaid Swisscom phone cards. These had been purchased in bulk, anonymously. But when investigators discovered through a wiretap on an intercepted call that "lasted less than a minute and involved not a single word of conversation" that they were on to an al Qaeda group, the agents tracked the users of the bulk purchase.[151] The result was the arrest of a number of operatives and the breakup of al Qaeda cells.

This example illustrates what the national security community realized years ago. In the age of electronic communications, wiretapping is a rich and fruitful investigative tool when you can get it, but the critical need to secure civilian infrastructure has the side effect that the contents of wiretapped communications will become increasingly inaccessible to investigators.[152] Instead, traffic analysis – who is communicating with whom – will become the more valuable tool. Traffic analysis can reveal an organization's structure, its membership, even the roles of its members, and can do so in a way that benefits the investigators without such negative impacts on the civilian infrastructure.

The actions of al Qaeda are ". . .on a scale approaching war, but they were committed by a loose, far-flung, nebulous conspiracy with no territories or citizens or assets that could readily be threatened, overwhelmed, or destroyed."[153] This war will likely see other destructive actions on the scale of September 11th or substantially worse. In the face of such a war, the United States needs to think carefully about the impact of the choices it makes. Many times, when the nation was threatened,

150. A case in point is the September 11th hijackers. Mohamed Atta described a nuclear facility as "electrical engineering" to his fellow pilots (NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 245). Khalid Sheikh Mohammed used the code of send "the skirts" to "Sally" to instruct another al Qaeda member to send funds to Zacarias Moussaoui. The targets were discussed as if the participants were students at a university: the Pentagon was "arts," the World Trade Center, "architecture," the Capitol, "law," and the White House, "politics." *Id.*, at 246, 248.

151. Don Van Natta, Jr, & Desmond Butler, *How Tiny Swiss Cellphone Chips Helped Track Global Terror Web*, N.Y. TIMES, March 4, 2004, at A1.

152. This realization is undoubtedly part of the reason for NSA acquiescence to the change in cryptographic export-control regulations in 2000.

153. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 348.

the response was to diminish citizens' freedoms. But, as the Church committee pointed out in the mid 1970s, "[p]ersons most intimidated by well not be those at the extremes of the political spectrum, but rather those nearer the middle. Yet voices of moderation are vital to balance public debate and avoid polarization of society."[154]

In the face of nihilistic threats from violent religious extremists, it is imperative to encourage voices from the middle. Moving to a surveillance society runs a serious risk of irreparably harming democratic participation. The security of the United States will face unprecedented challenges if ubiquitous surveillance has the effect of shutting down the voices of moderation from the immigrant communities. We cannot afford to take such a risk.

If you only have a hammer, everything looks like a nail. The FBI is primarily a crime-fighting agency rather than a crime-prevention one. Thus, the FBI has pressed for the extension of CALEA to VoIP. But this is the wrong tool at the wrong time, and its usage will create dangers rather than alleviate them.

## CONCLUSION

In considering wiretapping and other surveillance technologies, it is crucial to remember that the United States has two objectives: to save the lives of its citizens and not to lose independence and stability as a nation.[155] The application of CALEA to VoIP is not only an abrupt change in U.S. wiretap law, but also represents an anomaly in U.S. communications law.

From the very early days of the republic, the United States has treated communications as something of the people, for the people, and by the people. The Postal Act of 1792 established two fundamental principles: privacy of the mails – postal officials were not allowed to open mail unless the mail was undeliverable – and low rates for newspapers, thereby encouraging the dissemination of political information to the hinterlands. Thus the United States departed sharply from the governments of Britain and France, neither of which provided any such safeguards. Indeed, in Europe the postal service was a system of government surveillance. By contrast, the U.S. Post Office was seen as a facilitator of democracy and was one of the few strong federal institutions established in the nascent United States.[156]

The differences between European and U.S. communications systems extended to the development of new technologies. While in

154. INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, *supra* note 25, at 291.

155. HEYMANN, *supra* note 130, at xi.

156. PAUL STARR, THE CREATION OF THE MEDIA 3 (2004).

Europe, the telegraph system was a mechanism of state security,[157] that did not occur in the United States. In Europe, the telegraph system was government owned;[158] in the U.S., privately. In Europe, the adoption of new communications systems was slower and less geographically extensive; the major cities were connected, but not so the small towns and rural areas.[159] In America , small towns and rural areas enjoyed all the benefits of new communications systems.

The fact that the United States spanned a continent is a partial explanation for the rapid development of new communication systems; it was simpler to achieve integration in one nation than in many with competing regulatory systems. Other factors were at work as well, including the deeply held conviction that the spread of knowledge would aid in success the nation's democratic values. But a bedrock reason for the growth of telecommunications in the United States is the privacy afforded to communications. This spawned trust in the use of these communication systems, and a growing dependence on them.[160]

Nonetheless, the government can still read citizens' mail. Spying on the mails was a sufficient problem that in 1825 Congress felt obliged to address it. The Church Committee uncovered numerous instances of law enforcement and intelligence agencies reading private mail without a search warrant,[161] but the law has always been on the side of privacy. The 1825 Postal Act[162] made prying into another person's mail illegal. In 1878,[163] the Supreme Court ruled that the government could not open first-class mail without a search warrant. The FBI's efforts on CALEA undermine a 220 year tradition in this country of safeguarding privacy in communication systems.

The negative effects of applying CALEA to VoIP will ripple though the public and private sectors of America. It poses risks to the economy through the potential loss of corporate information. U.S. national security is threatened through the potential enabling of cost-effective massive intelligence gathering. There is a risk to the freedom of U.S. citizens. This echoes the risks Europeans faced because of the Echelon network. Echelon is an eavesdropping network run by the U.S., U.K., Australia, Canada, and New Zealand, that targets civilian

157. In order to conduct surveillance, European governments typically banned the use of ciphers. *See id.* at 159.

158. In Britain, the telegraph was initially private, but in 1870, Gladstone's government bought the private lines. *Id.* at 168.

159. *Id.* at 227.

160. *Id.* at 228.

161. A Resolution to Establish a Committee to Study Government Operations with Respect to Intelligence, S. Res. 21, 94th Cong. 62, 107 (1975).

162. Act of March 3, 1825, 4 Stat. 102.

163. Ex Parte Jackson, 96 U.S. 727 (1878).

communications;[164] its existence became public in the late 1990s. When that occurred, European governments sought to secure their private-sector communications and they liberalized their cryptographic export-control policy (so that the E.U. nations would be able to purchase security equipment from one another). The private sectors' need for communications security outweighed national-security and law-enforcement needs to conduct domestic wiretaps. The United States liberalized its cryptographic export-control policies shortly afterwards.

To law enforcement, it may seem obvious that wiretap laws should automatically be updated with each change in communications technology. Looking at the issues more broadly, this is far from clear. Wiretap laws were passed at particular times to satisfy particular sets of problems. As technology and society change, so must our laws. Society's security needs are not enhanced by requiring that VoIP implementations be CALEA-compliant. Rather, the CALEA requirements applied to the Internet are likely to cause serious harm to security, industrial innovation, and the political efforts in the war against violent Islamic fundamentalists. Among the first principles of security should be: "First, do no harm." The proposed CALEA requirements do not pass this test, and should not be approved.

164. Duncan Campbell, *Interception 2000: Development of Surveillance Technology and Risk of Abuse of Economic Information*, Report to the Director General for Research of the European Parliament, Luxembourg (April 1999), *available at* http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm.

# ADVENTURES IN SOFTWARE LICENSING: SCO V. IBM AND THE FUTURE OF THE OPEN SOURCE MODEL

ANDREW LAFONTAINE *



* Andrew Lafontaine is a J.D. candidate at the University of Colorado (2006).

## INTRODUCTION

People write for many reasons. Some for pleasure, others for money. An author wishing to profit from their work must find some way to limit access to that work to customers willing to pay for the privilege.[1] To accomplish this, authors typically employ a two-pronged strategy of copyright and license. The copyright prong imposes a statutory prohibition on the copying, use, or modification of the work without the copyright holder's permission.[2] The license prong is a contractual grant of that permission, subject to a set of restrictive terms designed to prevent the licensee from diluting the copyright holder's monopoly.[3] By lifting copyright prohibitions in exchange for money, this arrangement (which I label the "proprietary model") allows the author to earn a profit from their creation, which in turn incentivizes them to produce new works. The proprietary model of copyright and restrictive license is particularly prevalent in the software industry: companies like Microsoft license their programs to end users for a fee, using the proceeds to pay for the development of the next version of "Windows" or "Office."

Recently, however, another model software development known as the "free/open-source software" (F/OSS) movement has emerged to challenge the dominance of the proprietary model. This new model turns traditional notions of limited access on its head by inviting interested programmers from all over the world to freely copy, share, and modify each other's work.[4] Thanks in no small part to the advent of the Internet,[5] numerous projects have sprung up to develop F/OSS

1. PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 1.14.1 (3d ed. 2005).

2. 17 U.S.C. § 106 (2004).

3. The restatement describes a license by stating: "In a broad sense, the word 'license' is used to describe any permitted unusual freedom of action. It may be used to describe privileges to carry on businesses or to practice callings not otherwise permitted." RESTATEMENT OF PROP. § 512 cmt. a (1944).

4. Software development based on the free sharing of code is not new—during the early days of the computer era, code sharing was a regular practice in programming hotspots like AT&T's Bell Laboratories and in academia. However, it became increasingly rare as these institutions started to recognize the potentially enormous value of the software they produced.

5. Writing about the Linux Project, Columbia Law Professor Eben Moglen noted that: "[T]he Internet made it possible to aggregate collections of programmers far larger than any commercial manufacturer could afford . . . in a development project ultimately involving more

applications, often with the express purpose of competing with their commercially developed counterparts. Anyone may volunteer to participate in these projects in whatever capacity they desire; those who make contributions to such projects are rarely paid for their services, and the resulting products may be freely used by anyone. This approach has several advantages, not the least of which is that the presence of many sets of eyes ensures that software "bugs" (errors or glitches in the coding process) will be quickly discovered and corrected.[6]

F/OSS development has attracted a great deal of support and media buzz in recent years, yet despite all this attention the movement remains difficult to define precisely. F/OSS advocates are not of one mind—there is a great deal of disagreement about things as basic as the meaning of terms like "free" and "open." However, one thing that is widely agreed on is that the best way to promote the unfettered use and widespread distribution of code is to avoid restrictions on access to source code wherever possible — a position anathematic to the proprietary model. As important as this is to the open source model, F/OSS development is not synonymous to placing the code in the public domain. As I will explain below, F/OSS is typically distributed under a license which has been specially crafted to ensure that the code remains accessible long after it has left the developer's hands.

One especially important piece of F/OSS, which will be the focus of this paper, is the Linux operating system (OS).[7] Originally begun as a research project, Linux is widely seen as a successor to the venerable Unix OS, a proprietary system on which it is based. Although highly regarded for its power and stability, Unix fractured into a number of incompatible variants in the 1970s and 1980s, making development difficult.[8] By providing a single platform on which to standardize, while at the same time maintaining the familiar conceptual structure of Unix, the Linux project has been a great success.

---

than one million lines of computer code — a scale of collaboration among geographically dispersed unpaid volunteers previously unimaginable in human history." Eben Moglen, *Anarchism Triumphant: Free Software and the Death of Copyright*, FIRST MONDAY (1999), http://www.firstmonday.org/issues/issue4_8/moglen/index.html.

6. In his seminal paper, The Cathedral and the Bazaar, open source advocate Eric Raymond coined a phrase which has become the open source movement's unofficial mantra—"Given enough eyeballs, all bugs are shallow." Eric Raymond, *The Cathedral and the Bazaar, in* THE CATHEDRAL AND THE BAZAAR (Feb. 06, 2006) (unpublished manuscript, available at http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/).

7. Linux was and continues to be developed under the Free Software Foundation's "General Public License" (GPL), endowing it with a special feature known as "copyleft." While Linux is by no means unique in this respect, it should be pointed out that copyleft embodies the tenets of a particularly strident branch of open source philosophy.

8. *See* James V. DeLong, *The Enigma of Open Source Software (Version 1.0)*, 11.8 PROGRESS & FREEDOM FOUND. 12 (2004), http://www.pff.org/issues-pubs/pops/pop11.8opensource.pdf.

Recently however, a controversy has arisen between IBM, one of the major backers of Linux, and a small software company named SCO. As holder of the copyrights for one of the many Unix variants, SCO has sued IBM for allegedly inserting copyrighted code into Linux, an action strictly prohibited by IBM's Unix license agreement with AT&T (SCO's predecessor in interest.

Linux is widely seen as the greatest achievement of the F/OSS model, so this litigation raises a number of interesting questions. What is the likelihood of a SCO victory? What are the consequences for the Linux project if SCO is victorious? Are other open source projects vulnerable to similar challenges? This paper seeks to provide answers to these questions. My position is that while allegations of copyright violation in theory present a serious threat to open source projects like Linux, SCO is unlikely to prove wrongdoing in this particular litigation. I also argue that just as open source developers should not be allowed to take proprietary code without authorization (as is being alleged in the Linux suit), proprietary developers should not be allowed to appropriate the hard work of their open source counterparts. The open source movement's adoption of strategies like the General Public License (GPL) will help ensure that it is not put at a competitive disadvantage vis-à-vis proprietary software.

This paper is structured as follows. Section I sets out the basic principles of copyright and licensing, explaining the mechanics of the law and the concepts of original and derivative works. Section II describes how these copyright and licensing schemes are put to use by the proprietary and open source models, with particular focus on the specific provisions of the GPL. Section III traces the origin of the Unix and Linux operating systems, each of which represent a practical application of the two software models. Section IV covers the specific aspects of the current litigation between SCO and IBM, starting with a list of SCO's allegations, continuing with a discussion of license terms constraining IBM, and concluding with an analysis of IBM's position. Finally, Section V discusses the implication of this suit for the future of open source development, as well as the importance of the GPL in maintaining a level playing field between the open source and proprietary models.

## I. COPYRIGHTS AND LICENSING

### *A. The Basics*

The U.S. Constitution grants Congress the power to "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."[9] For authors, Congress has provided the ability to protect unique writings through the mechanism of copyright. Under federal law, no one except the copyright owner may reproduce, prepare derivative works based on, or distribute copies of copyrighted works.[10] These rights attach to "original works of authorship fixed in any tangible medium of expression"[11] and are vested initially in the author of such works.[12]

Due to the prohibitions set forth by copyright law, a non-copyright holder who wishes to reproduce, distribute, or prepare derivatives of a copyrighted work can only do so by obtaining the copyright holder's permission.[13] This is commonly accomplished through the mechanism of a license, which is a contract allowing the licensee to take certain actions that would otherwise be prohibited by copyright law.[14] Once granted, any action specifically provided for by the license will no longer be in violation of copyright; however, actions not provided for are still prohibited.[15] While some licenses grant the licensee virtually unrestricted access to the work,[16] it is more common for a license to selectively lift only certain copyright restrictions and leave others in place. The license may, for example, allow the creation of verbatim copies but not derivative works, or the preparation of a derivative work but not its distribution.

As a contract, a license can take just about any form the parties desire, so the grant of rights is often conditioned on the licensee's acceptance of other terms. While these terms commonly specify how the licensee may use the licensed item, they are by no means limited to this. A license might require the licensee to pay a fee for each copy of the work they make, or promise not to display the work in certain ways, or even (to give a somewhat ridiculous but theoretically possible example) shave her head before she is granted the right to use the work under license.[17]

---

9. U.S. CONST. art. I, § 8, cl. 8.

10. *See* 17 U.S.C. § 106 (2004).

11. *Id.* at § 102.

12. *See id.* at § 201.

13. *See id.* at § 106.

14. "A license is, in legal contemplation, merely an agreement not to sue the licensee for infringement." DAVID NIMMER & MELVILLE B. NIMMER, NIMMER ON COPYRIGHT § 10.01 n. 73.1 (Lexis Ed. 2004) (hereinafter NIMMER).

15. "[I]n the absence of clear evidence of a contrary intent, where an assignee has prepared the assignment, rights not expressly granted will often be held to be reserved by the assignor." NIMMER, *supra* note 14, at §10.08. Even though Nimmer refers to an assignment of copyright rather than a license, the principle is basic to contract law and applies in both contexts.

16. For instance, the BSD license allows the licensee to use, modify, and/or redistribute the code, subject only to a warranty disclaimer and a requirement that copyright notices be retained. *See infra* note 81.

17. A real world example of licensing terms so harsh they border on the absurd are those

A valid license only protects the licensee from copyright infringement if two conditions are met. First, the licensee must not act outside the scope of her license. As explained above, any action not specified in the license is still barred by copyright law. Second, she must observe any and all license provisions.[18] If the license is granted on certain terms, failure to comply with those terms may automatically revoke the license.[19] For this reason, license terms are vitally important, since revocation puts the licensee in the same position she would have been in had she never obtained the license in the first place—she is no longer shielded from the prohibitions of copyright law and any further use, distribution, or modification of the licensed work is illegal. It also means that copyright violation often goes hand-in-hand with breach of contract.[20]

### *B. Computer Software*

Software is available in two forms: source code and object code. Source code is the form in which software is originally written — it is human readable such that a programmer can understand it and modify it if she wishes.[21] Object code is a machine readable form that the source code must first be translated (or "compiled") into before it will run on a computer.[22] A programmer who hopes to make useful modifications to a piece of software must have access to its source code, and it is very difficult (if not impossible) to re-translate object code back into source code.[23] Proprietary software publishers, who rely on limited access for their business model, consider their programs' source code to be the crown jewels of their intellectual property and guard it jealously. They typically only distribute their programs in object code format, and forbid

---

once used by a company called Man's Best Friend Software. Its products, marketed to dog breeders and kennel owners, required the licensee to not to publish "derogatory statements" about the company, its products, or its employees. In addition, the terms required that the licensee "agree" that such statements would cause the company to suffer inestimable harm. In lieu of a trial or hearing on damages, they were obligated to pay a fixed amount of $10,000 for each derogatory publication. *See* Edward Foster, *The Worst Sneakwrap Agreement*, *at* http://www.gripe2ed.com/scoop/story/2004/3/4/84017/93009 (last visited Mar. 19, 2005).

18. *See* NIMMER, *supra* note 14, at § 10.15.

19. If the violation consists of a failure to satisfy a condition precedent to the grant of the license, the work was never effectively licensed in the first place and hence copyright violation is automatic. Alternatively, when dealing with license covenants that are not conditions precedent to the grant of a license, the license may provide for automatic revocation upon a breach by the licensee. *See id.*

20. *See id.*

21. *See* Wikipedia, Source Code, http://en.wikipedia.org/wiki/Source_code (last visited Mar. 26, 2005).

22. *See id.*

23. *See* Wikipedia, Decompiler, http://en.wikipedia.org/wiki/Decompiler (last visited Mar. 26, 2005).

users from attempting to de-compile or reverse engineer their program. The open source model, on the other hand, gets its namesake from the fact that this code is available to all.

Computer software is rarely bought and sold outright. Someone who buys a piece of boxed software from a store (or over the Internet) has in all likelihood purchased a license granting them the right to make a copy of the program to use on their own computer, on the condition that they agree with a specified set of terms. The typical proprietary license prohibits the licensee from making unauthorized copies of the software for distribution, while the typical open source license expressly allows the licensee to distribute copies freely.[24]

### 1. The Special Problem of Derivative Works

Software is frequently licensed not only for its usefulness as a standalone product, but also for the purpose of creating derivative works. A derivative work is nothing more than a recasting, transformation, or adaptation of one or more preexisting works.[25] The popular treatise *Nimmer on Copyright* states: "Copyright in a derivative or collective work covers only those elements contained therein that are original with the copyright claimant."[26] This means that two sets of rights exist in a derivative work. Copyright for the underlying elements of the original work remain with the original author, while copyright for the new contributions belong to the derivative author.[27] For this reason, the original author may not claim copyright in the new contributions, since she did not write them, but she may still claim copyright in the elements of the underlying work that the derivative contains.

Computer programs are a fertile ground for the creation of derivative works. Rather than writing a new program from scratch, it is often much easier to take existing code and modify it to provide new functionality.[28] One need look no further than popular applications such

24. As noted in section III(B)(ii), *infra*, some open source licenses provide that any redistributions *must* include the source code, while others make this optional.

25. *See* H.R. REP. No. 94-1476, at 57 (1976); *See also* 17 U.S.C § 101 (2004). Note that a derivative work is different from a collective work, which applies to items "such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole." 17 U.S.C. § 101.

26. NIMMER, *supra* note 14, at § 3.04.

27. This of course assumes that the derivative author has obtained permission from the original author to create a derivative work in the first place. An unauthorized derivative author has no right to create a derivative work. *See* 17 U.S.C. § 106 (2004).

28. As Eric Raymond puts it: "Good programmers know what to write. Great ones know what to rewrite (and reuse)." Eric Raymond, *The Mail Must Go Through*, *in* The Cathedral and the Bazaar (unpublished manuscript, available at http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ar01s02.html)

as Adobe Acrobat (currently in its seventh incarnation) or the Microsoft Office suite of programs (eleventh) to see this process in action. In copyright terms, each is a derivative of the previous version.[29]

Derivative works can be created in two ways. The first (and more straightforward) way occurs when someone adds to or modifies an existing work. This scenario occurs all the time in computer programming. A developer might start with a piece of code which is useful for completing certain tasks, but which does not quite fulfill her needs, and add and subtract code until it does.

The second method for creating derivative works is far more complex, and may be unique to the world of software. A completely original piece of code might be considered derivative if it interacts heavily with a pre-existing program, such as where one software module invokes the use of another.[30] This commonly occurs in the context of software "libraries," which, although not free-standing executables themselves, contain subprograms and helper data that other programs can utilize.[31] Depending on how a program invokes a copyrighted library, it might be considered a derivative work for the purposes of copyright law.[32]

### 2. Sublicensing

The author of a derivative work who wishes to distribute it as a standalone product may not do so unless they have the permission of the

---

(discussing his own experience improving email clients).

29. Note that in these examples, the party doing the updating also happens to be the copyright holder. However, in theory there is no reason why "Acrobat 8" or "Office 12" could not be released by a third party (assuming of course that they had proper authorization).

30. For an excellent discussion of this confusing but important topic, see David McGowan, Legal Aspects of Free and Open Source Software (Oct. 5, 2004) (unpublished manuscript, *available at* http://www.law.umn.edu/uploads/images/253/McGowanD-OpenSource.rtf; DeLong, *supra* note 8, at A1. Although this understanding of derivative is controversial, that has not stopped the Free Software Foundation from taking such a position. *See* Free Software Foundation, Frequently Asked Questions about the GNU GPL, http://www.gnu.org/licenses/gpl-faq.html (last visited Feb. 06, 2006).

31. See Wikipedia, Library (computer science), http://en.wikipedia.org/wiki/Shared_library (last visited Mar. 21 2006); BookRags.com, Software Libraries Summary, http://www.bookrags.com/sciences/computerscience/software-libraries-wcs.html (last visited Mar. 23, 2006).

32. As the preamble to The Free Software Foundation's "Lesser GPL" (LGPL) points out: "When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library." Free Software Foundation, GNU Lesser General Public License, http://www.gnu.org/licenses/lgpl.html. (last visited Mar. 14, 2006). Software libraries are an extremely important programming tool, and this rigid rule can create complications when dealing with certain "copyleft" provisions found in the standard GPL (set out in greater detail below). In recognition of this fact, the LGPL was created to allow open source developers the option of allowing proprietary programs to link to their libraries without running afoul these provisions. *See id.*

original author. Even though the derivative author holds the copyright for their contributions to the work, copyright for the underlying elements still rests with the original author. Permission is commonly obtained through a special form of license known as a sublicense, whereby the original author (the sublicensor) grants the derivative author (the sublicensee) permission to distribute a work in which she only holds partial copyright. Like any other license, a sublicense can set the terms on which this permission is granted, and it is common for these terms to affect the way the sublicensee distributes the derivative work to third parties. For example, if X sublicenses code from Y for the purpose of creating a derivative work, Y's sublicense agreement may dictate some or all of the terms on which X may license the derivative to Z.

## II. OPEN SOURCE VERSUS PROPRIETARY SOFTWARE

### *A. Two Alternative Models of Software Development*

Copyright law is premised on the idea that the creation of written works is driven by the pursuit of profits[33]—profits which the author derives from his ability to act as gatekeeper to his work.[34] Without this control, authors would be unable to make money off their creations and would lose their motivation to produce new ones.[35]

Combined with restrictive licensing terms, copyrights enable authors to sell limited rights to copy their work without giving up their monopoly status. In this proprietary model of development, copyrights are strictly enforced and the right to copy, use, or distribute code is granted only for a price. The more rights granted, the higher the price. Moreover, authors keep a tight grip on their work by crafting detailed licensing agreements to ensure that the rights granted under it extend no further than the immediate licensee. Sublicense agreements enabling the distribution of derivative works may require additional payment.

Over the past decade or so, a growing number of computer programmers, technology enthusiasts, and scholars have begun to

33. To quote Samuel Johnson, "No man but a blockhead ever wrote, except for money." JAMES BOSWELL, THE LIFE OF SAMUEL JOHNSON, L.L.D 19 (G. B. Hill ed., Oxford: Clarendon Press 1934).

34. Note that a copyright holder's ability to control access is not perfect. Copyright does not prohibit someone from reading a copyrighted book (or even selling it to someone else after they have done so)—only from copying or distributing it. However, in the context of computer software, the ability to copy is synonymous with access as a practical matter. Software is useless until it has been copied from the medium on which it has been distributed (such as a CDROM) to the machine were it will be run. The same goes for code available over a network such as the internet.

35. *See generally* Andrew Beckerman-Rodau, *Are Ideas Within The Traditional Definition of Property?: A Jurisprudential Analysis*, 47 ARK. L. REV. 603 (1994).

question whether this approach is the best way to maximize the output and value of creative work.[36] Restricting the ability to copy, modify, and distribute software may allow the copyright holder to extract the maximum amount of profit from their work, but that does not always guarantee the highest quality product.[37] Recently there has been a great deal of interest and participation in collaborative software development projects, characterized by wide distribution of code and freedom for users to copy, modify, and distribute it as they wish.[38] This drive toward collaborative development is often referred to as the open source movement and the term F/OSS refers to programs developed under the open source banner. As noted earlier, code sharing has been around since the dawn of the computer era, but this new movement stands apart both in its purposeful approach and its global reach.

F/OSS development projects are best conceived of as being structured as concentric rings: those with greater interest and willingness to commit more time occupy the center, while dabblers remain at the fringes.[39] This amorphous form is in keeping with the general egalitarian and equalitarian ideals of the movement, although some have suggested these structures are much more hierarchical in practice.[40] F/OSS projects have traditionally been supported by volunteer efforts, but an untold amount of money and programmer time has been contributed by commercial enterprises as well — IBM alone has committed over 200 programmers and invested over one billion dollars to the Linux project.[41]

---

36. *See* Yochai Benkler, *Coase's Penguin, or, Linux and the Nature of the Firm*, 112 YALE L.J. 369 (2002).

37. Few issues arouse as much passion as the dispute over whether the F/OSS model or the proprietary model produces "better" software. Part of the problem is there is no single yardstick to measure this by. F/OSS programs are notoriously user-unfriendly, but at the same time, they are more customizable to the user who knows what they are doing. Gauging by the number of software bugs is similarly problematic. In their 2005 year-end index, Cyber The US Computer Emergency Readiness Team identified 812 Windows operating system vulnerabilities, compared with 2328 for Unix/Linux operating vulnerabilities. *See* Cyber Security Bulletin 2005 (Dec. 29, 2005), *available at* http://www.us-cert.gov/cas/bulletins/SB2005.html. However, a 2004 report published by the online journal The Register noted a marked imbalance in the relative severity of the vulnerabilities and concluded that Linux was more secure. *See* Nicholos Petreley, *Security Report: Windows vs. Linux*, THE REGISTER, Oct. 22, 2004, http://www.theregister.co.uk/security/security_report_windows_vs_linux/. I do not take a position in this debate, and merely note that F/OSS advocates are united in their belief that their model is methodologically oriented to producing the highest quality code (even if it does not always deliver on that promise) and that the proprietary model necessarily subordinates this goal to the producer's bottom line.

38. *See* David McGowan, *Legal Implications of Open-Source Software*, 2001 U. ILL. L. REV. 241, 241-42 (2001).

39. *See* DeLong *supra* note 8, at 36.

40. *See* i*d.* at 34.

41. IBM CORPORATION, THE LINUX SERVICES OPPORTUNITY 16-17 (2003), http://www.ibm.com/partnerworld/pwhome.nsf/vAssetsLookup/ci_LinuxServices02.pdf/$File

There are probably as many different beliefs about the meaning of the term "open source" as there are programmers who espouse it. Some feel it is an embodiment of the American commitment to free expression, while others see it as a way to oppose monolithic software companies (Microsoft in particular) that currently dominate the world of computer software publishing.[42] For more than a few, it has taken on philosophical overtones, implicating issues that have as much to do with natural rights as they do with economic theory.[43] The very term "F/OSS" reflects this multiplicity of views: its most fervent adherents preach the gospel of "free software,"[44] while those advocating "open source software" are more pragmatically oriented.[45]

Despite all this, there are general characteristics of F/OSS that set it apart from proprietary software. In particular, the open source development model has different goals in mind from the proprietary code model. For all its ideological underpinnings, the primary objective of F/OSS development is quite functional: to produce the best code possible by allowing many individuals to participate in its creation. Software of all kinds is often plagued by coding errors called "bugs," which cause programs to malfunction or crash. A key component of the open source philosophy is that the best way to produce well written and bug-free software code is to allow a large number of programmers to tinker with it.[46]

In a typical open source project, a programmer, or a small group of programmers working together, posts unfinished program code to the Internet, where it can be downloaded by anyone. Other programmers and computer hobbyists then donate their time, completing unfinished sections and poring over the code trying to identify potential flaws. Working portions of code are run under adverse conditions to see if they fail, and if so, how. Not only does this process help uncover problems

---

/ci_LinuxServices02.pdf.

42. *See* Richard Stallman, *Is Microsoft the Great Satan?, in* PHILOSOPHY OF THE GNU PROJECT (2000), http://www.gnu.org/philosophy/microsoft.html.

43. *See* Richard Stallman, Why Software Should Not Have Owners, in PHILOSOPHY OF THE GNU PROJECT (2005), http://www.gnu.org/philosophy/why-free.html; Richard Stallman, *Why Software Should Be Free, in* PHILOSOPHY OF THE GNU PROJECT (1992), http://www.gnu.org/philosophy/shouldbefree.html.

44. Richard Stallman, one of the free software movement's most vocal advocates, puts things this way: "Free software' is a matter of liberty, not price. To understand the concept, you should think of "free" as in "free speech," not as in "free beer." Free Software Foundation, *The Free Software Definition, in* PHILOSOPHY OF THE GNU PROJECT (2004), http://www.gnu.org/philosophy/free-sw.html.

45. *See* Eric Raymond, Keeping an Open Mind (2003), http://www.catb.org/~esr/writings/openmind.html. Professor David McGowan provides a particularly clear picture of the dispute between firebrands like Stallman and more moderates voices like Raymond. *See* McGowan, *supra* note 38, at 261-63.

46. *See* Raymond, *The Cathedral and the Bazaar*, *supra* note 6.

that might otherwise have been overlooked, it allows a development project to draw on a much larger pool of expertise to find solutions. This process of peer review, well known in other fields, carries with it an added benefit captured by the old adage "many hands make like work."

It is the task of the open source developer to coordinate these efforts and keep everything running smoothly. While proprietary developers typically work in isolation, open source developers engage in a continuing dialogue with the programming community. Depending on the project, its coordinators may do very little of the actual coding themselves, instead devoting most of their time to managing logistics.[47] Code must be swapped back and forth, new contributions must be evaluated and incorporated, and the updated versions must be redistributed so the process can begin again.

Unlike the proprietary model of software development, the open source model is not explicitly geared toward inducing programmers to contribute with the promise of financial reward. While some programmers (such as those employed by commercial firms engaged in F/OSS development) do get paid for support, the model is premised on a number of non-monetary motivations. In a world where coding is seen as "a gift and an expression of art,"[48] some contribute out of a sense of altruism,[49] while others do it for the sheer enjoyment of solving complex problems and participating in something larger than themselves.[50] Professor Benkler, who has analyzed this issue at some length, breaks the motivations of F/OSS developers down into three categories: monetary rewards (which can be substantial for service-type contracts), intrinsic hedonic rewards (a sort of "play ethic"), and social-psychological rewards (pleasure from increasing one's status in the eyes of others through meaningful contributions to a project).[51] Whether these motivations are sustainable is an open question, but with open source projects like Linux still going strong after 15 years, they do not appear as transitory as some

47. In describing the work of Linus Torvalds (the creator of the open source Linux OS, discussed below) Eric Raymond comments that Mr. Torvalds' greatest contribution was not the Linux program itself, but his masterful use of the open source model. Says Mr. Raymond, "When I expressed this opinion in his presence once, he smiled and quietly repeated something he has often said: 'I'm basically a very lazy person who likes to get credit for things other people actually do.'" *Id.*

48. ERIC RAYMOND, OPEN SOURCE INITIATIVE, OSI POSITION PAPER ON THE SCO-VS.-IBM COMPLAINT (2004), http://opensource.org/sco-vs-ibm.html#id3153667.

49. *See* Richard Stallman, *Self Interest, in* PHILOSOPHY OF THE GNU PROJECT (2002), http://www.gnu.org/philosophy/self-interest.html; Alfie Kohn, *Studies Find Reward Often No Motivator*, BOSTON GLOBE, Jan. 19, 1987, *available at* http://www.gnu.org/philosophy/motivation.html.

50. *See* Eric Raymond, *Homesteading the Noosphere*, *in* THE CATHEDRAL AND THE BAZAAR (Aug. 24, 2000) (unpublished manuscript, available at http://www.catb.org/~esr/writings/cathedral-bazaar/homesteading/).

51. *See* Benkler, *supra* note 36, at 423-35.

would argue.[52]

### *B. Open Source Licensing*

As explained above, F/OSS programs are not typically placed in the public domain, but are instead distributed under special licenses designed to promote (rather than restrict) access to the underlying source code. Of these, the most well known, and probably the most controversial, is the GNU General Public License (GPL), under which Linux is distributed. A great deal of misunderstanding surrounds the GPL, so the next two subsections aim to clear up this confusion. I will first outline the basics of the GPL, then address some of its more exotic features, and finally explain the relationship between the GPL and the open source movement in general.

#### 1. The General Public License and "Copyleft"

The open source model requires unfettered access to source code in order to function. To this end, MIT researcher Richard Stallman created the GPL as a mechanism for software authors to provide such access.[53] Most licenses rely on the threat of copyright enforcement to keep works closed off, but in a form of legal jujitsu,[54] the GPL uses licenses to open works up to the world. Weighing in at around five single spaced pages of text, the GPL is short in comparison to many proprietary licenses.[55]

A quick glance at § 1 of the GPL reveals that it does not contain the types of restrictions contained in a typical proprietary license. It allows users to copy and distribute source code free of charge, so long as they provide to distributees a notice of copyright, a warranty disclaimer, and a full copy of the GPL license terms.[56] To facilitate improvement of programs, § 3 states that anyone who releases a program in object code format must also provide source code, or else make it easily accessible.[57]

If the GPL's purpose was merely to allow licensees to take code on generous terms, it would be rather uninteresting. However, the GPL takes the concept of open access a step further by incorporating a

---

52. For a more critical view of the longevity of the open source movement in general, *see* DeLong, *supra* note 8.

53. LI-CHENG TAI, THE HISTORY OF THE GNU GENERAL PUBLIC LICENSE (2001) http://www.free-soft.org/gpl_history/.

54. The term "legal jujitsu" comes from Benkler, supra note 36, at 446. This fighting style's art of using an opponent's momentum against them is an apt metaphor for the mechanics employed by the GPL.

55. FREE SOFTWARE FOUNDAITON, GNU GENERAL PUBLIC LICENSE (1991), http://www.gnu.org/licenses/gpl.html.

56. *Id.*

57. *Id.*

mechanism to ensure that open source software, once licensed, remains open. In § 2(b), the GPL provides that licensees may only take code if they agree to re-license any resulting work (provided they choose to distribute it) under the GPL as well.[58] In other words, any time code licensed under the GPL is distributed, either as a standalone product or as a component of a derivative work, the resulting product being distributed must itself be licensed under the GPL. Failure to do so will void the license, as provided in § 4.[59] In this way, the GPL perpetuates itself from program to program, creating a copy in each new iteration of the code originally licensed. Lest the licensee be caught unaware, this critical feature of the GPL is spelled out explicitly in § 6.[60]

A licensee who uses or modifies a GPL licensed program need not distribute it. If the licensee merely wants the program for their own personal use, they are not required to re-license it. The self-perpetuating features of the GPL are only triggered by the distribution of the program (or any modifications thereto).[61] Should a potential licensee be unwilling to re-license the program on the GPL's terms, § 5 instructs them not to license the program in the first place.[62]

To better understand how the GPL works, consider the following illustration. X creates a small piece of software and makes it available under the GPL. Y wants to incorporate this code into another program that she is working on, so she takes the code under the terms of the GPL, which authorizes derivative works. If Y chooses to distribute her new program containing X's code, Y's program must itself be released under § 2(b) of the GPL. Conversely, Y is barred from using X's code if Y does not want to distribute it under the GPL (perhaps she hoped to sell it for a profit).

The self perpetuating nature of the GPL has led some to label the license as "viral."[63] This viral nature is by design: it prevents programmers from incorporating a piece of code originally developed under an open model into a proprietary work. Many feel that allowing software developers to take from the programming community without giving back anything defeats the purpose of the open source model.[64] A

58. *Id.*

59. *Id.*

60. *Id.*

61. Because it allows the redistribution of the licensed work or a derivative of it, the GPL can be thought of as both a license and a sublicense rolled into one.

62. GNU GENERAL PUBLIC LICENSE, *supra* note 55.

63. Microsoft, which views open source software as a threat, is particularly fond of this somewhat loaded characterization. *See* Butt Wai Choon, *Not Quite an Open-and-Shut Case* (Mar. 2002), http://www.microsoft.com/malaysia/business/articles/linkpage3866.asp.

64. *See* Andrea Ciffolilli, *The Economics of Open Source Hijacking and the Declining Quality of Digital Information Resources: A Case For Copyleft*, 9 FIRST MONDAY (Sept. 2004), http://www.firstmonday.org/issues/issue9_9/ciffolilli/index.html.

non-viral GPL would be powerless to prevent the licensee from re-releasing the code under whatever onerous terms they wished. Since Stallman views freedom as an important component of open source software, a viral license is necessary to preserve that freedom for others: "Someone who uses your code in a non-free program is trying to deny freedom to others, and if you let him do it, you're failing to defend their freedom."[65]

Stallman coined the term "copyleft" to describe this protection of open source software through viral licensing. "Proprietary software developers use copyright to take away the users' freedom; we use copyright to guarantee their freedom. That's why we reverse the name, changing 'copyright' into 'copyleft'."[66] Software that has been copylefted is not only available to the public for free—its availability is forever protected through the unorthodox use of copyright law. This feature is the key innovation of the GPL.[67]

### 2. Does Open Source Necessarily Imply Copyleft?

While the GPL plays a vital role in the open source movement, a particular program need not be licensed under the GPL to be considered open source. The model includes any code developed under principles of free access and modification.[68] The particular licensing regime a developer chooses is merely a mechanism to put those principles into practice. There are literally dozens of standard licenses that an open source developer may choose from,[69] and if none meet the developer's needs, she is always free to write her own.

In an effort to explain just how a license should be structured to ensure the implementation of open source principles, a non-profit group called the Open Source Initiative (OSI) has promulgated a set of ten characteristics required of a license before software provided under it can be considered truly open source.[70] Copyleft figures prominently in this list. Though the status of copyleft as the *sine qua non* of the model is open to debate, it is widely regarded as a central feature of open source

65. Richard Stallman, *Why Copyleft, in* PHILOSOPHY OF THE GNU PROJECT (2003), http://www.gnu.org/philosophy/why-copyleft.html.

66. FREE SOFTWARE FOUNDATION, LICENSES (2005), http://www.gnu.org/licenses/licenses.html#WhatIsCopylefte.

67. At least one scholar has raised questions about the legal validity of copyleft provisions on privity of contract grounds. While the GPL has never been tested in court, McGowan argues that this is not a serious threat. *See supra* note 38, at 289-303.

68. Richard Stallman, *The Free Software Definition, in* PHILOSOPHY OF THE GNU PROJECT (2006), *http://www.gnu.org/philosophy/free-sw.html* (last visited Mar. 14, 2006).

69. *See* THE FREE SOFTWARE FOUNDATION, VARIOUS LICENSES AND COMMENTS ABOUT THEM, http://www.gnu.org/licenses/license-list.html (last visited Feb. 7, 2006).

70. THE OPEN SOURCE INITIATIVE, THE OPEN SOURCE DEFINITION (2006), http://www.opensource.org/docs/definition.php.

development.[71] The inclusion of copyleft terms in OSI's open source definition, combined with the fact that copyleft was pioneered by the GPL, helps explain the common misconception that code can only be considered open source if it is licensed under the GPL.

## III. PUTTING THE DIFFERENT DEVELOPMENT MODELS INTO PRACTICE: UNIX AND LINUX

Explaining the current controversy between SCO and IBM requires at least a basic understanding of the Unix development's extremely complex history. Unix does not have a unitary identity: [72] over the years, hundreds of variants have been developed, often by companies and institutions with very different agendas.[73] Portions of these variants have been mixed and mingled, and the result is a family tree that has aptly been described as a "plate of spaghetti."[74] This section only covers the few variants involved with Linux and the SCO v. IBM suit, but it is important to note that the disputes engendered by the incompatibility of the various Unix versions are a large part of Linux's *raison d'être*, and the agreements that came out of this period will have a great impact on the outcome of the present litigation.

### *A. General Background*

An operating system (OS) is a very important piece of computer software that controls the hardware of a specific data-processing system in order to allow users and application programs to make use of the system.[75] There are many different operating systems available today, of which the Microsoft Windows family of products is the most widely recognized. Not all OS's are created equal—they run the gamut in terms of functionality, stability, ease of use, and hardware requirements. However, for certain types of powerful computers, Unix is widely regarded as one of the best on the market.[76]

The first version of the Unix operating system was created by two

71. Stallman's views on the necessity of copyleft are not universally accepted in the open source community. However, as the elder statesman of the movement and one of its most outspoken advocates, his influence can hardly be overstated. *See* Stallman*, Why Copyleft, supra* note 65.

72. There is, however, a single Unix specification. *See* THE OPEN GROUP, THE SINGLE UNIX SPECIFICATION, VERSION 3 (2002), http://www.unix.org/version3/.

73. DeLong, *supra* note 8, at 12.

74. *Id.* at 11.

75. THE AMERICAN HERITAGE DICTIONARY (4th ed. 2000), *available at* http://www.bartleby.com/61/34/O0093400.html.

76. *See* Eric Raymond, *Origins and History of Unix, 1969-1995*, *in* THE ART OF UNIX PROGRAMMING (2003), http://library.n0i.net/linux-unix/art-unix-programming/ch02s01.html.

computer scientists at AT&T's Bell Labs in 1969.[77] Unix was not originally envisioned as a large scale project. Bell Labs had recently withdrawn from the consortium designing the MULTICS OS, and AT&T programmers Ken Thompson and Dennis Ritchie, who had grown used to the interactivity that MULTICS offered, sought to create a similar platform to run other projects they were working on.[78] As time went on, Unix became widely used within the Bell Labs programming community and the project eventually developed into a full-fledged OS.

Although originally developed on a DEC PDP-7, in 1973 Unix was completely rewritten in the high-level C programming language, allowing it to be recompiled to run on many different types of hardware.[79] Designing a new OS from scratch is a difficult thing, so the portability of Unix to different hardware configurations made it attractive to many outsiders. Under a 1956 antitrust agreement, AT&T was not allowed to commercialize its non-telephony IP, so thousands of entities were able to obtain Unix licenses practically for free.[80] Proprietary software was not seen as the tremendously valuable asset that it is today, so AT&T distributed the source code as well, sanctioning (and even encouraging) the development of Unix variants such as the Berkeley Software Distribution (BSD) at the University of California.[81]

### *B. IBM, AIX, and Sequent*

By 1984, attitudes towards proprietary software had changed, and AT&T's deregulation allowed it to try to capitalize on its Unix assets. As Unix grew in reputation, large companies like IBM, HP, and Sun became increasingly interested in running it on their own high end machines. This led to the creation of yet more variants, each by a different manufacturer. In 1985, IBM entered into a Unix licensing agreement with AT&T,[82] as well as a sublicensing agreement allowing it to license its Unix derivative called AIX to its customers.[83] IBM could

77. *See id.*
78. *Id.*
79. *Id.*
80. *See* DeLong, *supra* note 8, at 11-12.
81. Portions of BSD code made their way back into AT&T's Unix on at least one occasion. This greatly complicated matters when AT&T set about taking Unix proprietary, while BSD went open source. The resulting lawsuit, which was not settled until 1994, cast a pall of uncertainty over the entire project (and arguably contributed to the acceptance of Linux as an alternative). *See* Wikipedia, Berkeley Software Distribution, http://en.wikipedia.org/wiki/BSD (last visited Feb. 5, 2006).
82. Exhibit A to Second Amended Complaint, SCO Group v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-25-A.pdf [hereinafter SOFT-00015].
83. Exhibit B to Second Amended Complaint, SCO Group v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-25-B.pdf

now market a complete range of solutions consisting not only of a powerful computer system, but also enterprise level software[84] for them to run.

In September of 1999, IBM merged with Sequent Computer Systems, a company specializing in multi-processor computer design. Sequent had itself purchased a license for Unix and had developed a number of Unix-related software tools and programs (including its own homegrown Unix variant called Dynix/ptx). In the merger, IBM took possession of these assets, and in the process, bound itself to Sequent's license terms, which in some cases varied from its own.

### *C. The Convoluted History of the SCO Group*

#### 1. The Santa-Cruz Operation

Computer manufactures were not the only ones to create Unix variants. Seeing an opportunity to exploit an overlooked niche market, a small software firm named The Santa-Cruz Operation (Old SCO) created a variant of Unix in 1983 that would run on Intel processors.[85] Originally called SCO Unix, but later renamed to OpenServer, Old SCO's variant did not compete directly with the Unix variants developed by the likes of IPM and HP because the Intel processors of the time were still not used for high end computing. Nevertheless, OpenServer was moderately successful and the project gave Old SCO significant experience dealing with Intel-architecture processors.[86]

The emergence of Intel as the dominant processor manufacture in the mid-1990s greatly increased the demand for a server OS capable of running on these processors.[87] Old SCO now found itself in a very

[hereinafter SOFT-00015A].

84. Companies rely heavily on computer systems to run their back office (and often their front office) operations. Downtime can be tremendously costly, so software used in this environment is designed to be highly fault tolerant. The goal of an enterprise class computer system is "five nines" (99.999%) reliability, or an average downtime of less than five and a half minutes per year.

85. The SCO Group, Inc., *History of the SCO Group*, http://www.caldera.com/company/history.html (last visited Feb. 5, 2006).

86. Second Amended Complaint at 13, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-25.pdf [hereinafter Second Amended Complaint].

87. The 1990s witnessed the explosion of the market for desktop PCs, transforming Intel into a household name. Not content to stay confined to this area of the market, Intel began pouring its resources into improving its processor designs with the hope of expanding into the market for server processors as well. Over time, it increased the computing power of the x86 architecture until it was on par with high end processors. At the same time, it was able to maintain its cost advantage over these processors, for the first time making enterprise computers built with x86 processors an attractive choice. Intel's high price/performance ratio even convinced some manufacturers like HP and Compaq to abandon their own specialized

advantageous position, as their long history of working with Intel meant that they already had a mature Unix platform to deliver to customers. OpenServer offered the reliability of Unix on low cost (and now greatly improved) Intel processors.[88]

By comparison, other Unix variants were now much less attractive because they would only run on processors that were higher-priced, but which offered no better performance. IBM, perhaps sensing that the tide was shifting away from Unix running on its own brand of processors, entered into a joint-development program with Old SCO dubbed "Project Monterey" to design a Unix variant for Intel's next-generation processors.[89] This gave IBM access to Old SCO's copyrighted IP that allowed OpenServer to run on Intel.[90] Project Monterey was never completed and IBM pulled out of the agreement in May of 2001.[91]

#### 2. Novell, Caldera, and the SCO Group

In 1990, AT&T spun off its Unix business into a wholly owned subsidiary called Unix System Laboratories. Then, in 1993, a software company named Novell purchased the subsidiary, along with the Unix code and copyrights. In 1994, several Novell programmers left the company to form the startup Caldera, and in 1995 Novell sold the rights to Unix and UnixWare to Old SCO.[92]

Caldera spent several years distributing a version of the Linux OS before purchasing a number of Old SCO's assets in 2001. These assets included Old SCO's family of OpenServer products, as well as the rights to Unix that Old SCO had purchased from Novell. Finally, in 2002 Caldera changed its name to the SCO Group, giving us the company that we now know as SCO.[93]

### *D. Linux*

In many ways, programming culture of the 1960s and early 1970s mirrored the larger "free-love" spirit of the era. Places like AT&T's Bell Labs and MIT's Artificial Intelligence Lab brimmed with youthful

processor offerings and produce servers based exclusively on Intel chips. *See* Ian Fried, *HP plans to take Alpha to its Omega*, CNET NEWS.COM, Dec. 5, 2002, http://news.com.com/2100-1001-976211.html.

88. *See* Second Amended Complaint, *supra* note 86, at ¶ 48.

89. See Santa Cruz Operation Inc., Quarterly Report (Form 10-Q), at 28 (Feb. 15, 1999), *available at* http://www.groklaw.net/article.php?story=20040307113236 97 (last visited Feb. 5, 2006).

90. *See* Second Amended Complaint, *supra* note 86, at 13-14.

91. *Id.* at 14.

92. John C. Dvorak, SCO versus IBM and Linux: Timeline, http://www.dvorak.org/scotimeline/ (last visited Feb. 5, 2006).

93. The SCO Group, Inc., *supra* note 85.

energy and programmers collaborated widely.[94] By the 1980s, however, the communitarianism and pervasive code-sharing of the early days had been largely squelched by proprietary practices. In 1983, a group of programmers unhappy with this situation and led by Richard Stallman (who was particularly disheartened by the decline of the old ethos at MIT's AI Lab) formed the non-profit Free Software Foundation (FSF) to promote the creation of software under the open source model.[95] The Free Software Foundation has made many contributions to the open source movement, one of which is the so-called GNU project to create an open source alternative to Unix.[96]

A functioning OS requires a special software module called a kernel — a piece of code that directly interacts with the hardware. Even though the FSF never succeeded in creating one, a Finnish computer science student name Linus Torvalds was working independently on his own kernel at the same time as the FSF. Dubbed Linux, the kernel could be combined with a number of software components developed by the GNU project to create a fully operational OS.[97] Since its release under the GPL in 1991, the Linux project has received contributions from tens of thousands of programmers and software designers. Over time, Linux has grown into an extremely powerful and fully featured OS, representing to many the best example of what the open source model is able to accomplish.

## IV. THE SCO V. IBM LAWSUIT

### *A. SCO's Allegations*

By the end of the millennium, even large for-profit companies had

94. Eric Raymond paints a compelling picture of the programmers of the day: "Socially, they were young, exceptionally bright, almost entirely male, dedicated to programming to the point of addiction, and tended to have streaks of stubborn nonconformism — what years later would be called 'geeks'. They, too, tended to be shaggy hippies and hippie-wannabes. They, too, had a vision of computers as community-building devices…. Collaborative development and the sharing of source code was a valued tactic for Unix programmers." *See* Eric Raymond, *Origins and History of the Hackers, 1961-1995*, http://library.n0i.net/linux-unix/art-unix-programming/hackers.html (last visited Feb. 5, 2006).

95. FREE SOFTWARE FOUNDATION, OVERVIEW OF THE GNU PROJECT (2005), http://www.gnu.org/gnu/gnu-history.html.

96. Stallman's decision to go with Unix (as opposed to another OS) was shaped largely by practical considerations: "Unix is not my ideal system, but it is not too bad. The essential features of Unix seem to be good ones, and I think I can fill in what Unix lacks without spoiling them. And a system compatible with Unix would be convenient for many other people to adopt." *See* RICHARD STALLMAN, THE GNU MANIFESTO (2005), http://www.gnu.org/gnu/manifesto.html.

97. *See* Wikipedia, Linux kernel, http://en.wikipedia.org/wiki/Linux_kernel (as of Feb. 5, 2006).

taken notice of Linux. IBM in particular saw advantages in offering this OS to complement its enterprise class servers — it was functionally similar to the various Unix variants that its customers were used to, but could be provided without the costly licensing fees.[98] The cost of the OS typically constitutes a significant portion of the purchase price for an enterprise class server,[99] so IBM could undercut the competition by saying in essence, "buy our hardware and we'll throw in a free OS!" It may have lost some of the revenue it previously generated through AIX licenses, but presumably this was offset by an increase in hardware sales.[100]

In order for IBM's strategy to work, however, significant work had to be done to Linux to put it on par with traditional Unix offerings both in terms of stability and functionality. IBM had, after all, spent nearly 20 years refining its AIX operating system. Customers relied on various versions of Unix to run their "business-critical" applications, so a lower cost would be irrelevant if Linux could not meet the demanding requirements of the enterprise computing environment every bit as well as its proprietary competitors. IBM therefore pledged to help develop Linux by contributing to the project time, programmer talent, and most importantly, certain code assets it possessed.[101] It was these code contributions that formed the basis for the lawsuit from SCO.

As the ostensible owner of Unix copyrights, SCO was concerned that the code IBM was making available to Linux developers rightfully belonged to them. IBM may have had access to it through various license agreements, but these agreements explicitly prohibited any further distribution. In March of 2003, SCO terminated any rights IBM had to Unix and brought suit against them, alleging misappropriation of trade secrets, unfair competition, and breach of contract.[102] In addition, SCO mailed a letter threatening legal action to 1,500 companies using Linux as well.[103] SCO also sued two corporate Linux users (AutoZone and

98. *See* Second Amended Complaint, *supra* note 86, at 17.

99. For example, under IBM's original Unix license, AT&T changed $43,000 for the first CPU and $16,000 for additional CPU the software was run on. AT&T charged an additional $25,000 every time IBM sublicensed Unix (or AIX). Note that these are in 1985 dollars! *See* SOFT-00015, *supra* note 82.

100. SCO alleges a more sinister motivation behind IBM's change of heart. They argue that it was motivated by the company's recent shift away from a licensing revenue model to a service model — that IBM was no longer trying to make money by licensing AIX, but would instead make money from providing services to companies using any variant of Unix or Linux. Distributing Linux as a free replacement for Unix made sense, because it still allowed IBM to sell server hardware, while at the same time making it harder for other companies to make money by licensing their (non-free) versions of Unix. *See* Second Amended Complaint, *supra* note 86, at 19-24.

101. *Id.* at 20-25.

102. *See* Second Amended Complaint, *supra* note 86, at 32-64.

103. Exhibit I to Amended Counterclaims, SCO Group, Inc. v. IBM, No. 03-CV-0294

Daimler-Chrysler) for injunctive relief and damages,[104] presumably to make an example out of them.

SCO's complaint against IBM has since been amended twice, dropping the misappropriation of trade secrets cause of action and adding a copyright claim.[105] It is the copyright claim that is the focus of the remainder of this section. If SCO's allegations prove true, every version of the Linux kernel distributed since roughly the year 2000 is in violation of copyright, as is everyone possessing and using such a copy. However, despite the fact that the trial has now been going on for over two years, SCO has yet to produce the offending lines of code to substantiate its claims.

### *B. IBM's License Agreements*

Recall that IBM originally acquired its rights to Unix through a license from AT&T, and that it later created AIX as a derivative work to be distributed under a corresponding sublicense agreement. The contract licensing Unix from AT&T to IBM ("Software Agreement / SOFT-00015"), along with the sublicense agreement ("Software Agreement / SUB-00015A"), are perhaps the most important documents in the case. They set out the terms under which IBM may use Unix, as well as the rights it has to distribute, prepare derivative works, and sublicense AIX. With their acquisition of Sequent, IBM took over Sequent's portfolio of intellectual property assets. Many of these assets, such as Dynix/ptx were also based on code licensed from AT&T. In addition the licenses themselves, SCO and IBM have also filed with the court several amendments and a letter ("1985 Side Letter") modifying their arrangement.[106] I have reproduced below the most important terms of the various licenses along with a brief explanation of each section.

#### 1. SOFT-00015: IBM's Original Unix License

§ 2.01. AT&T grants to [IBM] a personal, nontransferable and nonexclusive right to use in the United States each [licensed software product (referring to Unix)] identified in the one or more Supplements

(D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-41-I.pdf.

104. For more information on these suits, *see* The SCO Group, Inc., *SCO v. AutoZone,* http://www.sco.com/scoip/lawsuits/autozone/index.html (last visited Feb. 5, 2006), *and* The SCO Group, Inc., *SCO v. Daimler Chrysler*, http://www.sco.com/scoip/lawsuits/daimlerchrysler/index.html (last visited Feb. 5, 2006).

105. Second Amended Complaint, *supra* note 86, at 50.

106. Exhibit 15 in Declaration of Jeremy O. Evans in Support of SCO's Memorandum in Opposition to IBM's Motion for Summary Judgment on Breach of Contract Claims, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-41-D.pdf [hereinafter Side Letter].

hereto, solely for [IBM's] own internal business purposes . . . Such right to use includes the right to modify such [licensed software] and to prepare derivative works . . . provided the resulting materials are treated hereunder as part of the original [licensed products].[107] Although not technically an amendment, the 1985 Side Letter ¶ A2 remarked that: "Regarding Section 2.01, we agree that modifications and derivative works prepared by or for you are owned by you. However, ownership of any portion or portions of [a licensed product] included in any such modification or derivative work remains with us."[108]

Section 2.01 is the basic grant of rights to Unix from AT&T to IBM. These rights include the ability to use Unix for IBM's internal business purposes, and to create derivative works. The side letter provides that portions of derivative works will be owned by their respective authors.

Sections 2.05 and 7.01 make clear that the license applies solely to IBM,[109] and strictly prohibits IBM from transferring any of the licensed assets in whole or in part.[110] However, § 7.06 as amended by the 1985 Side Letter ¶ A9 provides that while IBM may not disclose the licensed assets to anyone,

> [n]othing in this agreement shall prevent [IBM] from developing or marketing products or services employing ideas, concepts, know-how or techniques relating to data processing embodied in [the licensed products] subject to this Agreement, provided that [IBM] shall not copy any code from such [licensed products] into any such product.[111]

Finally, SOFT-00015 sets out the fee structure whereby IBM must pay AT&T based on the number of computers running Unix.[112]

### 2. SUB-00015A: IBM's AIX Sublicense

IBM is also constrained regarding AIX. As a derivative work based on Unix, AT&T conditioned AIX's distribution on certain terms set out in the sublicensing agreement SUB-00015A. Section 2.01 of the agreement grants IBM the right to furnish third parties with copies of the sublicensed product, so long as those parties agree to certain conditions.[113] In particular, third parties are prohibited from themselves

---

107. SOFT-00015, *supra* note 82, at 2.

108. Side Letter, *supra* note 106, at 2.

109. SOFT-00015, *supra* note 82, at 3.

110. *Id.* at 4.

111. *Id.*

112. To be more precise, the fees are based on the number of processors being used rather than the number of computers. This distinction is important because large computers often contain multiple processors.

113. SOFT-00015A, *supra* note 83, at 2-3.

redistributing the software. Just as in the license agreement, SUB-00015A also requires IBM to pay a fee for each copy of AIX it distributes.

#### 3. The Sequent License & Sublicense

Sequent, like IBM, licensed Unix from AT&T to create their Dynix/ptx variant. The terms of the license and sublicense were the same as those of IBM, since AT&T used a standard software license form for its products. Nevertheless, there is one crucial difference with regard to the two companies: the 1985 Side Letter between IBM and AT&T made several modifications to SOFT-00015, but there was no corresponding agreement between Sequent and AT&T. Thus, IBM had slightly more expansive rights to Unix than Sequent.

In particular, § 2.01 of AT&T's standard license agreement provides that any derivative works are to be treated as part of the original licensed works. Put another way, derivative works prepared by Sequent were subject to the same restrictions as the original. This adds a new wrinkle to the derivative works doctrine. Ordinarily, the author of an authorized derivative work can do whatever she likes with the new contributions she has made and the original author controls what is done with the original elements.[114] But the Sequent license could be interpreted to mean that AT&T's derivative works authorization is broader than copyright law, conditioned upon AT&T's control of all of Sequent's contributions. Read this way, even elements of Dynix/ptx that are completely original to Sequent would still subject them to the restrictions of the license agreement.

### *C. Analysis of IBM's Position*

#### 1. A Snarled Chain of Title

In 1995, Novell executed a contract filed with the court as the "Asset Purchase Agreement" (APA), in which it sold to Old SCO a number of Unix related assets. The APA is a rather lengthy document that sets out in detail just what was transferred. In § 1.1(a), it spelled out the sale to Old SCO of all "right, title and interest" in the items listed on a form labeled "Schedule 1.1(a)" which was attached to the APA.[115] It also included a list of certain assets *not* transferred, on a form labeled

114. *See* 17 U.S.C. §§ 102, 103 (2006).

115. Exhibit J to Defendant IBM's Answer to the Amended Complaint and Counterclaim-Plaintiff IBM's Counterclaims against SCO, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-41-J.pdf.

"Schedule 1.1(b)" which was also attached.[116]

Schedule 1.1(a) provided that included in the transferred assets were "[a]ll rights and ownership of Unix," as well as "all technical, design, development, installation, operation and maintenance information concerning UNIX and UnixWare, including source code . . . ."[117] Confusingly, however, Schedule 1.1(b), specifically withheld all copyrights and patents.[118] In 1996, Novell and Old SCO executed an amendment to the APA in a document labeled "Amendment 2." One of the effects of this amendment was to modify Schedule 1.1(b), so that it now excluded:

> All copyrights and trademarks, *except for the copyrights and trademarks owned by Novell as of the date of the Agreement required for SCO to exercise its rights with respect to the acquisition of UNIX* and UnixWare technologies. However, in no event shall Novell be liable to SCO for any claim brought by any third party pertaining to said copyrights and trademarks (emphasis added).[119]

What does this mean for the litigation? The amended APA would seem to say that SCO only owns the copyright to Unix if the copyright is required for SCO to "exercise its rights with respect to the acquisition of Unix."[120] But this, of course, begs the question: is the Unix copyright necessary for SCO to "exercise its rights?" If SCO does not own the copyright, then the entire case is moot.

Novell has, in fact, taken exactly this position. In May of 2003, it publicly asserted that SCO did not posses the copyright to Unix,[121] and, acting as the "true" copyright holder, purported to waive any and all claims regarding IBM's Linux contributions.[122] Immediately thereafter, SCO filed (yet another) suit against Novell for slander of title.[123] This unsettled matter could very well be determinative in the litigation between SCO and IBM, but until the court renders an opinion, the most anyone can do is speculate on the effect all this will have on SCO's claims.

---

116. *Id.*

117. *Id.*

118. *Id.*

119.Exhibit 29 to [Redacted] Memorandum in Support of SCO's Expedited Motion to Enforce the Court's Amended Scheduling Order Dated June 10, 2004, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://sco.tuxrocks.com/Docs/Amendment2.html.

120. *Id.*

121. Second Amended Complaint, *supra* note 86, at ¶ 19.

122. Exhibit K to Amended Counterclaim, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-41-K.pdf.

123. Complaint at 9, SCO Group, Inc. v. Novell, Inc., No. 04-CV-00139 (D. Utah filed Jan. 20, 2004), *available at* http://www.groklaw.net/pdf/Novell-0.pdf.

2. Amendment X: A Dead-End?

In its briefs to the court, IBM relies on an amendment to SOFT-00015 labeled "Amendment X" to support its claim that it may do whatever it likes with the code licensed from AT&T. This amendment was executed after AT&T sold Unix to Novell. The pertinent portion is § 1, which reads in part:

> [IBM] will have the irrevocable, fully paid-up, perpetual right to exercise all of its rights under the Related Agreements . . . Notwithstanding the above, the irrevocable nature of the above rights will in no way be construed to limit Novell's or SCO's rights to enjoin or otherwise prohibit IBM from violating any and all of Novell's or SCO's rights under this Amendment No. X, the Related Agreements, or under general patent, copyright, or trademark law.[124]

IBM's filings with the court have put particular emphasis on their "irrevocable, fully paid up, [and] perpetual" rights to Unix.[125] They claim that SCO may not terminate their rights under the license agreement because those rights are "irrevocable." However, I contend that IBM's emphasis on Amendment X does little to strengthen its defenses against SCO's allegations.

Amendment X does not expand any of IBM's rights under the license agreement and merely says that IBM's Unix license is no longer terminable by the copyright holder. Notwithstanding the perpetual and irrevocable nature of the amended license, IBM is still bound by its terms. If SCO is able to prove that IBM failed to abide by the license terms, such as those that prohibit revealing confidential source code to others, then IBM is in breach of contract. A license is a contract, so a party in breach of that contract may lose the protections it provides.[126] Without the protection of the license, further use of Unix-related IP would be in violation of copyright law. Since the second sentence of Amendment X § 1 says that SCO may prohibit IBM from violating its copyrights, IBM's reliance on Amendment X is misplaced.

A creative response to this argument might go something like this: even if IBM was in breach of contract, it can never actually lose its license since that license is irrevocable. This would render SCO's

---

124. Exhibit G to Defendant IBM's Answer to the Amended Complaint and Counterclaim-Plaintiff IBM's Counterclaims against SCO, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-41-G.pdf.

125. Answer to Amended Complaint and Counterclaim, SCO Group, Inc. v. IBM, No. 03-CV-0294 (D. Utah filed Mar. 6, 2003), *available at* http://www.groklaw.net/pdf/Doc-27.pdf.

126. *See* NIMMER, *supra* note 14, at § 10.15.

copyright claim moot because no matter how much it violated the license terms, it would still technically be covered by it. Since the license was always in force, copyright prohibitions would never be triggered.

However, this counter-argument fails for two reasons. First, it violates the spirit of the agreement by allowing IBM to breach its contract with impunity while leaving SCO without a remedy. Second, it is possible for IBM to be in copyright violation even without a direct breach of the license terms. Remember that a license only grants the rights to engage in a narrow spectrum of activities ordinarily prohibited by copyright. IBM is in violation if it acts outside the scope of these rights. The license certainly did not grant IBM the right to make unrestricted distributions of the Unix source code, so there is no way IBM could legally do so, perpetual license or not.

Careful analysis shows that Amendment X does not advance IBM's case despite its strong language. In the end, the legality of the Linux distributions turns on the nature of the code: if it is original to AT&T then it is subject to copyright, but if it was created in-house then IBM is off the hook.

### 3. A Better Response: IBM's Right to Create Derivative Works

IBM was granted the right to create derivative works for its own use by § 2.01 of the SOFT-00015 contract. The 1985 Side Letter further states that "we agree that modifications and derivative works prepared by or for you are owned by you. However, ownership of any portion or portions of [the licensed software products] included in any such modification or derivative work remains with us."[127] This parallels standard copyright law — each author is granted copyright in their respective contributions to a collective or derivative work.[128]

I believe that IBM's right to create derivative works is their salvation. As explained in Part II(A) of this paper, there are two sets of rights present in a derivative work: those of the original author and those of the new author. Assuming the new author has permission from the original author to create a derivative work (which the original author is of course free to withhold), the new author will hold copyright in their independent contributions to the derivative. As for the original author, they will retain copyright in the original elements still present in the derivative, *but not the new elements*.[129] The trick is separating the new elements from the old elements. Software code is highly modular, and it

127. Side Letter, *supra* note 106, at ¶ A2.

128. 17 U.S.C. §§ 102, 103 (2004).

129. 17 USC § 103(b) (2004) reads, in part: "The copyright in a compilation or derivative work extends only to the material contributed by the author of such work . . . ."

is possible that code originally written as a derivative could be useful as a standalone product with little or no modification. Since IBM only contributed certain sections of AIX to Linux developers, it is entirely possible that these sections contain only elements which they themselves created independent of the SCO code.[130] If so, they are completely within their rights to do so — SCO has no claim over these elements. Independent creation and modularity are key here. The code may have been a derivative in the sense that it interacted heavily with SCO code (much like a program would interact with a library), but in fact was created entirely at IBM. Even though this code was originally designed to work with code belonging to SCO, large portions might be modular enough so as to be functional with non-SCO code as well. If it turns out that IBM's contributions to Linux consisted entirely of independent, original, and modular code, then IBM has not breached its license terms. No breach of contract means no copyright violation, and SCO's case falls apart.

There are two potential hurdles to this defense. The first lies in the terms of the sublicensing agreement SUB-00015A, while the second has to do with the problem of Dynix/ptx contributions. As detailed in Sections IV(B)(1) and (2), SUB-00015A § 1.04 speaks about derivative works in a slightly different way than SOFT-0015A does. It defines the sublicensed product as computer programs "based" on software products licensed to IBM in SOFT-00015. This ambiguity is important, since AIX is certainly "based" on Unix. As we have seen, IBM-created code, when linked up with Unix code, constitutes a derivative work. Assuming the code is sufficiently modular to be decoupled from Unix code, IBM can argue that once decoupled, it is no longer derivative and IBM is free under the 1985 Side Letter to do with it as it wishes. If, on the other hand, the term "based" is substituted for "derivative," this decoupling is more difficult. Even decoupled, IBM's code is arguably still "based" on Unix, in the sense that linking with Unix was the original reason for its creation. The proper interpretation of these two terms is something that only a court can determine, but it is not readily apparent why a court would opt to read the term "based" more broadly than the term "derivative."

More troubling are the Sequent licensing terms set out in Section IV(B)(3), since arguably they *do* apply to any and all products based on the original version of Unix. A number of the items that SCO has

130. Defining the scope of derivative works in software is difficult and controversial. Some would argue that these additions are not derivative at all, but rather, completely original pieces of work. *See* Mitchell L. Stoltz, *The Penguin Paradox*, 85 B.U. L. Rev. 1439, 1441, 1449-51 (2005); Greg R. Vetter, *"Infectious" Open Source Software: Spreading Incentives or Promoting Resistance?*, 36 RUTGERS L.J. 53, 94-110 (2005).

alleged IBM contributed are software components originally developed by Sequent for Dynix/ptx under its own Unix license. Without knowing the actual lines of code in question, it is impossible to tell whether Linux does in fact contain elements of Dynix/ptx. If it does, then on its face, the distribution of these elements is in violation of the license.

This eventuality seems unlikely however. It seems unlikely the Unix derivative works right IBM negotiated in the SOFT-00015 and SUB-00015A licenses would be limited because of IBM's future purchase of the more restrictive Unix derivative works right in the Sequent license. In other words, the Unix derivative works rights of the SOFT-00015 and SUB-00015A licenses should supersede the more restrictive Unix derivative works right of the Sequent license. If not, the liability is still reduced as only Sequent-specific derived works suffer from this liability, so SCO will need to point these out.

## V. WHAT THIS MEANS FOR F/OSS DEVELOPMENT

Having seen an instance of litigation involving the two models of software development, what does this portend for the future of open source development (and Linux in particular)? I argue that while the Linux project is secure for the time being, the long term health of the model requires that F/OSS projects be seen as viable alternatives to their proprietary counterparts. To achieve this, an aggressive deployment of the GPL ensures that at the very least F/OSS projects do not start off at a disadvantage, while at the same time preserving the incentive structure that has served the model so well thus far.

### *A. Implications for Linux and Other F/OSS Projects*

Assuming that SCO produces specific lines of code that the court finds Linux infringes upon, the immediate effect will probably be quite small. Within the world of open source development, the Linux programming community is one of the largest and most active.[131] The offending code would eventually be rewritten independent from access to SCO's code, leaving the software immune from further intellectual property claims (at least by SCO).

IBM itself would be in hot water; SCO's complaint has asked for damages in excess of two billion dollars. But more damaging to Linux, and the open source movement as a whole, would be the effect an

131. While determining the exact number of contributors to a large F/OSS development project like Linux is difficult, a 2001 analysis of the Red Hat 7.1 Linux distribution revealed that it contained over 30 million lines of source code. The study estimated that under the proprietary model, the amount of programmer time this represented would be valued in excess of $1 billion. David A. Wheeler, More Than a Gigabuck: Estimating GNU/Linux's Size, http://www.dwheeler.com/sloc/ (last visited Mar. 14, 2006).

adverse decision would have on users — corporate users in particular. If Linux is indeed held to be an infringing work, each act of copying is an instance of copyright infringement. While SCO did not specify any specific legal action it was contemplating in the 1,500 letters it sent out, the penalties for companies using Linux could potentially be severe.

The SCO litigation raises the very real danger that users will be dissuaded from using Linux solely out of fear.[132] Even if the open source community were to produce a "clean room" version that could be verified from top to bottom as being free from proprietary code, this would take time to develop. In the interim, a company that wanted to be absolutely certain that it would not be liable for copyright infringement would have to migrate off the Linux platform. Migrating an entire company's computer infrastructure to a new operating system is extremely difficult, costly, and time consuming. Once the migration is complete, there is little incentive to migrate back to Linux. Few would be willing to risk getting "burned" again from some other challenge to open source.

Luckily, these dangers have not materialized as of yet; companies do not seem to be taking action one way or the other with regard to Linux. The suit against Daimler-Chrysler was dismissed,[133] while AutoZone has vigorously defended itself and the litigation has bogged down. With the IBM trial is currently scheduled for 2007, it may be some time before there are further developments.

Even if the Linux project is eventually vindicated, there is nothing to prevent this scenario from being repeated in the context of some other F/OSS project. Unless a developer writes all of their code from scratch, there is always the danger that their program will somehow be "tainted" by the presence of unauthorized code. This threat will probably never be fully neutralized given the cost of writing good code and testing it thoroughly and the incentive this creates for developers to reuse code.

When it comes to detecting the presence of unauthorized code, proprietary developers possess an informational advantage. Open source code is available for all to see, allowing proprietary developers to inspect it for infringement. Conversely, the secret nature of proprietary code means that an open source developer may not know that they are in

132. The practice of spreading FUD (fear, uncertainty, doubt) about Linux has a long and storied history among its competitors. *See* Eric Raymond, The Halloween Documents, http://www.catb.org/~esr/halloween/index.html (last visited Mar. 23, 2006). Professor McGowan believes that the current litigation is part of a larger rhetorical battle being waged against the open source model, and that this battle will be decided largely without regard to the legal merits of the various claims being made. David McGowan, *SCO What?* (Univ. of Minn. Law Sch. Legal Studies Research Paper Series, No. 04-9, June 6, 2004), *available at* http://ssrn.com/abstract=555851.

133. SCO Group, Inc. v. DaimlerChrysler Corp., No. 260036 (Mich. Ct. App. Jan. 31, 2005), *available at* http://www.groklaw.net/pdf/DC-8.pdf.

possession of infringing proprietary code until it is too late.

It is often unclear how code finds its way out of a proprietary product. Perhaps a lowly programmer was particularly proud of it and posted it to an internet bulletin board without the consent of their employer. Perhaps it was copied out of a derivative work by a licensee of the derivative's author, who mistakenly believed that they possessed the proper license. Or perhaps it was ripped straight out of a copyrighted work by a large corporation and illegally donated to an open source developer — as SCO alleges occurred at IBM.

Going forward, developers would be well advised to avoid code of uncertain origin. But what about F/OSS programs created before the current age of heightened awareness? No developer wants their first notification of infringement to be through service of process. Unfortunately, there is no easy way to determine software pedigree ahead of time.

### *B. Long Term Viability*

Success breeds success. In the F/OSS context, the more widely a program is used, the larger the pool of potential contributors. For programmers, there are psychological rewards associated with being a part of a successful project, such as increased standing in the eyes of other programmers and a heightened sense of accomplishment in a job well done. Working on a credible alternative to a proprietary product also awakens a natural sense of competition and instills F/OSS contributors with a purpose — beat Microsoft! — that working on a hopeless also-ran does not. People strive harder when the race is close.

F/OSS projects have flourished in part because they provide a creative outlet for the participants; indeed the open source movement is an outgrowth of this previously underserved need. Yet network effects which are so profoundly at work in this environment can operate in a negative fashion too. Just as success breeds success, a loss in momentum breeds attrition. The model is heavily dependant on non-monetary rewards to motivate contributions, so anything that interferes with that incentive system risks alienating a large segment of participants. When the Linux suit was first announced, what struck fear into the hearts of open source advocates was not that it threatened to make the software permanently unusable, but that the psychic injury to contributors that a SCO victory would have caused might have been irreparable to the project's continued existence.

The GPL plays an important role in preserving the continued vitality of F/OSS projects. First, it ensures a level playing field during development, increasing these projects' chances of being credible alternatives to proprietary software. Given that proprietary developers do

not want F/OSS developers to be able to free ride off of their work (and will go to court to prevent this), basic fairness dictates that they should not be allowed to appropriate F/OSS code for themselves. Open source licenses without copyleft provisions do nothing to prevent this eventuality; only the GPL can prevent a proprietary developer from incorporating open source code into his own project.[134] This is probably less of an issue in "clash of the titans" match-ups such as Linux versus Windows; Microsoft has more than enough resources to develop its own code without needing to "mooch" off F/OSS developers. However, not all programs are Microsoft Windows, and for smaller software projects, it can be difficult for an open source developer to get ahead if his new ideas are constantly in danger of being co-opted by proprietary "competitors."

Second, by preventing this unwelcome appropriation, the GPL preserves the open source model's incentive system. To quote Harvard Law professor Jonathan Zittrain, the self-perpetuating aspects of copyleft can be seen "as a quid pro quo for using and improving upon those works, to compel others to contribute to that pool any improvements they make and wish to release. . . . [If those works] stood to be proprietized by some future party, current contributors might be tempted to hold back their contributions to the common project."[135]

Proprietization of F/OSS code subverts the purpose of the entire open source movement, and particularly affects those who strongly identify with the tenets "free software." The open source movement can ill-afford to lose this important segment of its membership.

## CONCLUSION

The open source model is a welcome alternative to the proprietary model of software development. While each possesses its own set of strengths and weaknesses, choice is rarely a bad thing. Because there is much interest in the long term viability of F/OSS projects, SCO's suit against IBM has generated a great deal of consternation among Linux users. Luckily for these users (and open source developers in general), I

134. Even a programmer who is not philosophically opposed to keeping code secret—or who does not mind seeing someone else take their free code and incorporate it into a proprietary work—is still likely to favor measures that keep the playing field level because this gives open source alternatives the best chance of coming out on top (thereby "sticking it to" proprietary naysayers). As Eric Raymond puts it: "The typical pragmatist attitude is only moderately anticommercial, and its major grievance against the corporate world is not 'hoarding' per se. Rather it is that world's perverse refusal to adopt superior approaches incorporating Unix and open standards and open-source software. If the pragmatist hates anything, it is less likely to be 'hoarders' in general than the current King Log of the software establishment; formerly IBM, now Microsoft." Raymond, *Homesteading the Noosphere*, *supra* note 50.

135. Jonathan Zittrain, *Normative Principles For Evaluating Free and Proprietary Software*, 71 U. CHI. L. REV. 265, 279 (2004).

believe they have little to fear from this litigation because SCO will struggle in proving IBM did not have the right to contribute its derivative and independent code to Linux. That said, the risk of unauthorized code use is still present, so developers are advised to use caution. More broadly, the future health of the open source model requires that F/OSS programs be seen as legitimate alternatives to proprietary software. By employing innovative strategies like the GPL, F/OSS developers not only ensure that they compete on a level playing field with proprietary developers, but they also preserve the incentive structure necessary to motivate future contributions.