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

ISSN: 1543-8899

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

Subscriptions

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

International volume subscriptions are available for $50.00.

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

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

Manuscripts

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

Cite as: 5 J. ON TELECOMM. & HIGH TECH. L. __ (2007).

JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

Volume 5 *Spring 2007*

THE UNIVERSITY OF COLORADO SCHOOL OF LAW

FACULTY, 2006-07

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.

THE HONORABLE 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.

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

VICTOR FLEISCHER, *Associate Professor of Law.* B.A., Columbia University; J.D., Columbia University.

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

PIERRE J. SCHLAG, *Associate Dean for Research and Byron White Professor of 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 of Law.* B.A., University of Toronto; LL.B., University of British Columbia Faculty of Law; J.S.D., Cornell Law School.

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

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

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

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

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.

Research and Clinical Faculty

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

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

SHELDON E. FRIEDMAN, *Clinical Professor*. B.S., B.A., LL.B., 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

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

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

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

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

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

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

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

Legal Writing and Appellate Advocacy Faculty

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

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

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.

KEVIN L. DORAN, *Research Associate, Energy Law and Policy; International Environmental Law*.

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.

THE HONORABLE HANK BROWN, *President, University of Colorado*. B.A., J.D. University of Colorado; LL.M. George Washington University.

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

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.

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.

LORNA DWYER, *Professor of Law, Los Andes University, Bogata, Columbia.* J.D., Santo Thomas University.

CONSTANCE TROMBLE EYSTER, *Member, Hutchinson Black & Cook, LLC*. A.B., Dartmouth College; 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.

CRAIG C. GARBY, *Partner, Rothgerber Johnson & Lyons LLP, Denver, Colorado.* B.A., University of Colorado; Graduate Research, Waseda University, Tokyo, Japan; M.P.A., Cornell University; J.D., Stanford University.

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

NATALIE HANLON-LEH, *Partner, Faegre & Benson LLP, 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.

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.

LAWRENCE MACDONNELL, *Of Counsel, Porzak Browning & Bushong LLP*, B.A., University of Michigan; J.D. University of Denver; Ph.D. Colorado School of Mines.

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

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

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

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

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

PATRICK S. RYAN, *Faculty Director, Interdisciplinary Telecommunications Program, University of Colorado*. B.A., M.B.A., Monterey Institute of International Studies; J.D., University of Texas; M.B.L.-H.S.G., Universitat St. Gallen; Ph.D., Katholieke Universiteit Leuven.

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., J.D., University of Wyoming; LL.M, University of Denver.

NINA Y. WANG, *Associate, Faegre & Benson LLP.* A.B. Washington University; J.D. Harvard University.

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

LISA WAYNE, *Attorney at Law.* B.A., University of Colorado, J.D., Pepperdine University College of Law.

FROM THE EDITOR

This issue marks a new endeavor for the *Journal on Telecommunications & High Technology Law*. Quantitatively, we are increasing our annual run to three issues per volume. Qualitatively, however, we aim to steer JTHTL into new territory; we hope that issue three will come to focus on the life sciences, with a particular emphasis on the law, economics, and policy of the industry.[1] Bioscience companies received one third of the venture capital raised in Colorado in 2006, and the Fitzsimons Biobusiness Incubator (as well as its board members) continues to drive the bioscience industry to new heights in our state.[2] It therefore seems fitting to focus our editorial lens on an industry so crucial to the local and national economy, not to mention the educational environment at the University of Colorado.

With that goal in mind, this issue contains a student note focused on bioscience in criminal law and two articles on intellectual property issues, as well as a third article on telecommunications, our traditional strike zone. Patrick Haines embraces the DNA Fingerprint Act of 2005, defending the legality of a statute that requires any person arrested for a federal crime to provide a DNA sample. Professors Sicker and Ohm, along with Shannon Gunaji, reflect upon the "analog hole" in digital rights management schemes, and present their empirical study of consumers' willingness to pay for copies made via the analog hole. Chris Riley, editor-in-chief of the *Yale Journal on Law and Technology*, examines the impact of the Supreme Court's *Sony* and *Grokster* decisions on software innovation policy, while Robert Litan and Hal Singer round out the issue with their contribution to a long line of leading articles on network neutrality that have appeared in this publication.[3]

As I write this, snow is falling in Boulder, and the board of editors for volume five approaches the academic finish line. During the past 11 months, we produced high quality scholarship faster and cheaper, and

---

1. As Emerson said, "[a] foolish consistency is the hobgoblin of little minds[.]" RALPH WALDO EMERSON, ESSAYS 57 (1904).

2. *See* Will Shanley, *Colo. Firms See Venture Capital Drop*, DENVER POST, Jan. 23, 2007, at C4; ONBIOVC, ONBIOVC 1Q07 SUMMARY (Apr. 3, 2007), http://ab.rubenstein.googlepages.com/OnBioVCSummary1Q07.pdf.

3. *See* Neutrality Law Resources: Debates and Scholarship on Network Neutrality, http://www.neutralitylaw.com (last visited Apr. 13, 2007) (compiling articles from the *Journal on Telecommunications & High Technology Law* and the Silicon Flatirons Program concerning network neutrality).

with fewer resources than our predecessors. We created an amazing website, neutralitylaw.com, which compiles all of our scholarship and conference videos on network neutrality policy. We even added a third issue, which has served its intended purpose as a transitional device between graduating third-year editors and the incoming board. Finally, we moved from an asbestos-ridden office in the basement of the old law school into a shared space on the third floor of the brand-new Wolf Law Building, integrated our back office with that of the University of Colorado Law Review and the Colorado Journal on International Environmental Law and Policy, and increased our subscriptions by ten percent. In other words, the board of editors of volume five can depart CU Law with pride.

These accomplishments are due to the outstanding efforts of Kevin Bell, James Crowe, Preston Johnson, and Darlene Kondo. Becky Farr, Patrick Haines, Ryan Howe, and Justin Pless likewise helped to produce a wonderful crop of student notes and comments. Mark Walker, Danny Sherwinter, and Todd Spanier had to share an office with me this year, and for that alone they deserve an award. In the end, however, I know that David Wilson, Todd Blair, Carin Twining, and Michael Beylkin will put us all to shame when they take the helm of volume six.

Brad Bernthal, Dale Hatfield, the Silicon Flatirons Program advisory board, Paul Ohm, and Phil Weiser also deserve special thanks. In reviewing the 2L student note submissions for volume six, the value of Brad and Dale's help in that regard is self-evident. Paul served as an admirable pinch runner for Phil this year, offering a seemingly endless supply of support and advice, going so far as to take a hit (and a walk) by joining the Law School's Student Fee Committee, which helps to fund this publication. And then there's Phil.

With regards to Phil, it is enough to say that he exemplifies the following precept:

יְהִי כְבוֹד תַּלְמִידְךָ חָבִיב עָלֶיךָ כְּשֶׁלְּךָ, וּכְבוֹד חֲבֵרְךָ כְּמוֹרָא רַבְּךָ, וּמוֹרָא רַבְּךָ כְּמוֹרָא שָׁמָיִם[4]

Along with the board of editors, I am pleased to offer this, the third and final issue of the fifth volume of the *Journal on Telecommunications & High Technology Law*.

Micah Schwalb
Editor-in-Chief

---

4. "Let the honor of your student be as precious to you as your own; and the honor of your colleague as the reverence due your teacher; and the reverence towards your teacher as your reverence for heaven." PIRKEI AVOT 4:15.

JOURNAL ON
TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

Volume 5 *Spring 2007*

CONTENTS

ARTICLES

STUDENT COMMENT

UNINTENDED CONSEQUENCES OF NET NEUTRALITY REGULATION

ROBERT E. LITAN* & HAL J. SINGER**

Policymakers are in the midst of an active debate over how best to accelerate the build-out of next-generation broadband networks. The U.S. economy has a significant economic stake in the outcome. It is increasingly apparent in the global economy linked together by the Internet that the future competitiveness of individual firms, and indeed entire economies, depends heavily on state-of-the-art networks. Next-generation broadband networks will be significantly more expensive than earlier versions. In the U.S. alone, the required investment to deploy such networks ubiquitously could exceed $140 billion. This investment will not occur unless those who supply the funds for it are compensated with a rate of return commensurate with the risk. In virtually all private-sector markets, firms that undertake investments have sufficient freedom to fashion the way in which they offer the products and services those investments make possible, and to price them in ways that meet demands and optimize returns. In the broadband Internet access market, however, advocates of proposed network neutrality ("net neutrality") regulation would restrict those planning to build out next-generation networks from these freedoms.

This paper examines one particular aspect of the "net neutrality" proposals: "non-discrimination" requirements relating to the provision of network quality of service ("QoS") to content providers. The paper concludes that such requirements, however innocuous they may seem, would be detrimental to the objectives that all Americans seemingly should want—namely, the accelerated construction of next-generation networks, and the lower prices, broader consumer choices, and innovations these networks would bring. The paper also concludes that under the best of circumstances, even if networks are significantly upgraded in the presence of net neutrality rules, the proposed non-discrimination provisions would provide incentives for those who would build and operate networks to offer "blended" QoS levels that are "too high" for some applications and "too low" for others. Mediocrity in broadband service is hardly an objective that policymakers in the United States should be trying to achieve.

---

* Senior Fellow, Economic Studies Program, The Brookings Institution and Vice President of Research and Policy, Kauffman Foundation

** President, Criterion Economics. We thank Robert Hahn and Evan Leo for helpful comments, and AT&T Inc. for research funding. The views expressed here are solely our own.

I. INTRODUCTION AND POLICY BACKGROUND

There is a broad consensus among policymakers that it is in the economic interest of the United States and its citizens that broadband penetration not only increase, but that the next generation of "high bandwidth" broadband be built out as rapidly as possible. More advanced broadband networks not only will make the services and products offered over the Internet more attractive, but will accelerate innovation in the development of new content. There is one issue, however, which up to now has divided those who want a better and faster Internet: the assertion by some that consumers and content providers would be better off if the communications companies that will build the next-generation networks are subject to a series of "neutrality" restrictions. In particular, proponents of various forms of "net neutrality" argue that broadband network providers be prohibited from discriminating in any way in the provision of quality of service ("QoS") to content providers.

This seemingly innocuous requirement in fact would have far-reaching—and we believe demonstrably negative—implications for the U.S. broadband industry. In this introduction, we preview the issues and then examine them in-depth in subsequent sections. We show how net neutrality requirements very likely would lead to net mediocrity in service offerings, an outcome totally inconsistent with the desire of many end-users of the Internet and those offering many goods and services on the Internet. Such an outcome is clearly inconsistent with the objectives of policymakers to make the U.S. broadband networks and services the world leaders in technology, utilization, and customer value. There is much investment at stake in designing the optimal regulatory framework, as next-generation broadband networks will be significantly more expensive than earlier versions. In the United States, the cost per home of deploying these advanced facilities could reach $1,400,[1] which implies that the required investment to deploy next-generation networks ubiquitously could exceed $140 billion (equal to the product of $1,400 per home and 100 million U.S. homes).

A. The ABCs of QoS

Broadband networks are used to move data packets from one place on the network to another. Unfortunately, many bad things can happen to data packets as they travel across the Internet. For example, a packet may get dropped, may incur a delay, or may suffer from jitter. QoS is one antidote to such bad things. Internet applications differ in the extent to

1. VERIZON COMMC'NS INC., FIOS BRIEFING SESSION 40 (2006), *available at* http://investor.verizon.com/news/20060927/20060927.pdf (estimating net capital expenditure per home to be $1,434 for its planned FiOS deployment).

which they are "QoS-needy"—that is, the level of QoS they require to function properly.[2] The most popular QoS-needy applications include streaming multimedia, online gaming, voice-over-Internet protocol ("VoIP"), video teleconferencing, alarm signaling, and safety-critical applications such as remote surgery. In the future, there will be even more QoS-needy applications. Under the current regulatory regime, a content provider can contract for a certain level of QoS from an access provider by entering into a Service Level Agreement ("SLA"), which provides a guaranteed level of QoS.

Under a broad definition, QoS supplied by an access provider can take many forms and can be provided at several different layers of a broadband network, from the transmission media layer ("layer one") through the IP packet layer ("layer three") all the way up to the service application layer. For example, an access provider can cache external Internet content within its network in close proximity to end-users, thereby providing an enhanced performance for content providers and their customers. Access providers can also offer content providers enhanced hosting services at Internet data centers ("IDCs") deployed at strategic nodes of their networks, thereby bypassing possible intermediate bottlenecks between content servers and customer locations. A business with multiple office locations can purchase a virtual private network ("VPN") to secure a preferred level of service for all of its data traffic (including Internet-bound traffic) that traverses the access provider's network.

Alternatively, QoS can be defined more narrowly to apply only to layer three capability built into the routers and the IP packet header. For example, a customer (including content providers) could buy Internet access with QoS options that would ensure that any traffic the customer marked as high priority would get priority treatment on the access provider's network. Or a VoIP provider can buy QoS to give its packet streams preference through an access provider's network.

B. Various Forms of "Net Neutrality"

Non-discrimination typically implies similar treatment for similar types of customers or traffic. For example, a non-discrimination or duty-to-deal requirement could mandate that if an access provider offers a certain level of QoS to one content provider at a given price, then it must offer the same level of QoS to all content providers at the same price. Alternatively, an access provider could be prohibited from charging more

2. The technical term for content that requires a certain level of QoS to function properly is "inelastic." Because the term elastic has a different meaning for an economist (namely, the sensitivity of demand for a service in response to a change in prices or income), we use the term "QoS-needy" for ease of exposition.

for a steady 50 kbps VoIP stream than for a steady 50 kb/s gaming application where the QoS requirements—that is, the incremental cost of providing QoS to the two content providers—are the same.[3]

But under each of the net neutrality bills in Congress, non-discrimination in the supply of QoS means something more extreme: if a broadband provider offers enhanced QoS to any individual content provider, *then it must offer the same enhanced QoS to all content providers for free*. The apparent motivation for such a restriction is to stymie efforts by any content provider to secure enhanced QoS from broadband providers, and instead to force all contracting for QoS to occur between broadband providers and end-users.[4] These bills generally do not distinguish between broadband services offered by access providers versus those offered by backbone networks, and they would presumably impose their net neutrality restrictions on both types of networks. Because of the unquestioned lack of market power in backbone services—for example, even a combination of the backbone of Verizon (including MCI's backbone) and AT&T (including the old SBC's backbone) would account for less than 30 percent of all Internet traffic, while combining the top seven backbones would account for roughly 65 percent of total Internet traffic—there is certainly no competitive virtue in imposing non-discrimination restrictions on backbone networks.[5] If this non-discrimination objective has any sense, it must relate to competitive issues in the access network. Hence, we discuss the implications of net neutrality for broadband access networks.

One net neutrality bill in the House, H.R. 5273, explains in its preamble that "a network neutrality policy based upon the principle of nondiscrimination is essential to ensure that broadband telecommunications networks, including the Internet, remain open to independent service and content providers."[6] With respect to end-users, H.R. 5273 would require that access providers "not block, impair, degrade, discriminate against, or interfere with the ability of any person

3. *See* Jon M. Peha, *The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy*, 34TH TELECOMM. POL'Y RES. CONF., at 17 (2006), *available at* http://web.si.umich.edu/tprc/papers/2006/574/Peha_balanced_net_neutrality_policy.pdf.

4. *See*, *e.g.*, *Net Neutrality: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 2 (2006) (statement of Lawrence Lessig, Professor of Law, Stanford Law School) ("To oppose access tiering [with content providers], however, is not to oppose all tiering. I believe, for example, that consumer-tiering should be encouraged. Network providers need incentives to build better broadband services. Consumer-tiering would provide those incentives.").

5. *See* Opinion of the Cal. Attorney Gen. on Competitive Effects of Proposed Merger of Verizon Commc'ns, Inc. & MCI, Inc., Cal. PUC Dkt No. 05-04-020 (2005), *available at* http://www.cpuc.ca.gov/word_pdf/news_release/49697.pdf. Thus, this analysis will focus only on the potential effects of imposing such restrictions on access networks.

6. H.R. 5273, 109th Cong. § 2(10) (2006) [hereinafter H.R. 5273].

to utilize their broadband service."[7] With respect to content providers, the bill would require that access providers "not discriminate *in favor of itself* in the allocation, use, or quality of broadband services or interconnection with other broadband networks."[8] In addition, access providers must ensure that unaffiliated content is delivered "at least equal to the speed and quality of service that the *operator's* content, applications, or service is accessed and offered, and without interference or surcharges on the basis of such content, applications, or services."[9] Finally, "if the broadband network provider prioritizes or offers enhanced quality of service to data of a particular type, [then it must] prioritize or offer enhanced quality of service to all data of that type (regardless of the origin of such data) *without imposing a surcharge* or other consideration for such prioritization or quality of service."[10] The bill defines a "broadband network provider" as "a person or entity that owns, controls, or resells, facilities used in the transmission of a broadband service and includes any affiliate, joint venture partner, or agent of such provider."[11] Note that there is no distinction between an access provider and a backbone provider—both backbone networks and access networks are comprised of "facilities used in the transmission of a broadband service." Hence, enhanced QoS provided at either the access level or the backbone level for a fee by an access provider would presumably be prohibited under this bill. Indeed, because the bill defines "broadband service" as "two-way transmission capability that . . . enables the user to access content, applications, and services,"[12] the bill could implicate *any* supplier along the bit stream, including a supplier of enhanced QoS like Akamai. An important exception to the non-discrimination provision contained in H.R. 5273 is that access providers may "offer varying levels of transmission speed or bandwidth,"[13] presumably to both end-users and content providers. Nonetheless, under H.R. 5273, access providers cannot offer different levels of QoS, and they cannot set a price for enhanced QoS.

Another "net neutrality" bill, S. 2360, similarly would prevent an access provider from discriminating in the provision of QoS to content providers,[14] and it would ban any charges for QoS.[15] But S. 2360 also

7. *Id.* § 4(a)(2).
8. *Id.* § 4(a)(5) (emphasis added).
9. *Id.* § 4(a)(6) (emphasis added).
10. *Id.* § 4(a)(7) (emphasis added).
11. *Id.* § 4(e)(1).
12. H.R. 5273, 109th Cong. § 4(e)(2) (2006).
13. *Id.* § 4(b)(2).
14. S. Res. 2360, 109th Cong. § 4(a)(6) (2006) (An access provider must "treat all data traveling over or on communications in a non-discriminatory way").
15. *Id.* § 4(a)(4) (An access provider must "offer communications such that a subscriber can access, and a content provider can offer, unaffiliated content or applications or services in

would deny an access provider from discriminating against either a content provider or end-user with respect to bandwidth.[16] Another net neutrality bill, S. 2917, would prevent an access provider from discriminating against a content provider with respect to bandwidth or QoS.[17] Access providers could offer prioritization to end-users but could not impose a fee for such service.[18]

In December 2006, the FCC approved an $86 billion merger between AT&T and BellSouth, two large providers of DSL service in non-overlapping territories.[19] Two FCC commissioners would not approve the merger unless AT&T promised to abide by several conditions, one of which concerned network neutrality. Under the network neutrality condition, AT&T agreed to conduct business in accordance with the principles set out in the FCC's Policy Statement for a period of 30 months.[20] In particular, the condition required that AT&T not provide or sell any service that "privileges, degrades or prioritizes any packet transmitted over AT&T/BellSouth's wireline broadband Internet access service based on its source, ownership or destination."[21]

Three provisions in the merger commitments narrowed the scope of the network neutrality conditions. First, the requirement did not apply to service available only to enterprise customers, including VPN and managed-IP services.[22] Second, the requirement applied only from "the network side of the customer premise equipment up to and including the Internet Exchange Point closest to the customer's premise . . . ."[23] This implies that the merged entity has the right to offer prioritization to content providers at portions of its network just beyond the network side of the customer premise equipment such as edge services.[24] Third, the

---

the same manner that content of the network operator is accessed and offered, without interference or surcharges").

16. *Id.* § 4(a)(2) (An access provider must "not discriminate in favor of itself or any other person, including any affiliate or company with which such operator has a business relationship in—(A) allocating bandwidth").

17. S. Res. 2917, 109th Cong. § 12(a)(4)(A) (2006) [hereinafter S. 2917].

18. *Id.* § 12(a)(5).

19. Press Release, FCC, FCC Approves Merger of AT&T Inc. and Bellsouth Corporation (Dec. 29, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-269275A1.pdf.

20. Letter from Robert W. Quinn Jr., Senior Vice President, AT&T Servs. Inc. to Marlene H. Dortch, Sec'y FCC, in Response to *Notice of Ex Parte Communication* in Review of AT&T Inc. and BellSouth Corp. Application for Consent to Transfer of Control, WC Dkt. No. 06-74 (Dec. 28, 2006), *available at* http://www.fcc.gov/ATT_FINALMergerCommitments12-28.pdf.

21. *Id.* at 8.

22. *Id.* at 9.

23. *Id.* at 8.

24. *See*, *e.g.*, *FTC Able to Address Broadband Discrimination, Majoras Says*, TR DAILY, Jan. 9, 2007 ("The network geography to which this applies is between the end user and the first network server reached . . . . Things that happen upstream [under agreements with

commitment does not apply to AT&T's Internet Protocol television service, which is expected to compete against cable television and direct broadcast satellite service.[25]

FCC Chairman Kevin Martin supported the AT&T-BellSouth merger, but not the concessions relating to network neutrality. In his joint statement of dissent with Commissioner Deborah Taylor Tate, Martin supported the merger for enabling a wider array of IP-enabled services for customers and faster speed of broadband deployment in the BellSouth region.[26] But Martin argued that the condition involving network neutrality was not merger-related and he expressed concern that the network neutrality condition might deter facilities investment, thus creating a major obstacle to the FCC's key goal of broadband deployment to all Americans.[27] Martin also explained that the provision would in no way bind the FCC in future decisions regarding Internet policy.[28]

Following on the heels of the merger approval and AT&T's merger commitments, on January 6, 2007, Senators Byron Dorgan and Olympia Snowe reintroduced network neutrality legislation.[29] According to Senator Snowe, "[t]he reintroduction of this legislation and the FCC's imposition of net neutrality conditions as part of the merger are significant victories in the fight to ensure nondiscrimination on the Internet."[30] The reintroduced bill was identical to the original bill introduced in 2006. Thus, the bill would prevent *any* contracting between access providers and content providers. That provision would greatly expand the common meaning of "non-discrimination," which typically would require that an offering to an affiliated content provider be extended to non-affiliated content providers.[31] Moreover, the reintroduced bill appeared to ignore the limitations in the scope of the network neutrality provisions contained in the AT&T merger commitments.

---

carriers] are fair game.").

25. Quinn, *supra* note 20, at 9.

26. *See* Press Release, FCC Joint Statement of Chairman Kevin J. Martin and Commissioner Deborah Taylor Tate in AT&T Inc. and BellSouth Corporation Application for Transfer of Control, WC Dkt. No. 06-74 (Oct. 29, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-269275A2.pdf.

27. *Id.* at 2.

28. *Id.*

29. *Dorgan, Snowe Take Another Stab at Net Neutrality Legislation*, TR DAILY, Jan. 9, 2007.

30. *Id.*

31. *See*, *e.g.*, *'Nondiscrimination' Will Become Focus of Net Neutrality Debate, Martin Says,* TR DAILY, Jan. 10, 2007 (explaining that the FCC traditionally has meant by "'non-discrimination' that a carrier had to offer the same deal to all customers, but some net neutrality advocates seem to use the term to mean that broadband Internet access providers cannot charge content providers" any price).

Thus, the reintroduced network neutrality legislation is more restrictive than the AT&T merger commitments in the sense that the legislation forbids an access provider's contracting with content providers at *any* portion of the network, whereas the AT&T merger commitments tolerate an access provider's contracting with content providers beyond the Internet exchange point nearest to the customer. This is not to say that the merger commitments relating to network neutrality will not impose costs on AT&T and society. Efficient contracting for prioritization that could occur between "the network side of the customer premise equipment up to and including the Internet Exchange Point closest to the customer's premise"[32]—and the associated welfare gains that could flow from such contracting—will be prohibited under the merger commitments. The mere fact that, at the time of merger approval, such contracting had yet to occur at that portion of the access provider's network (yet had occurred beyond that portion of the network) does not imply that such contracting could not occur in the subsequent 30 month period.

C. A Guide to the Debate

According to net neutrality proponents, any surcharge for enhanced QoS would impair an unaffiliated content provider's ability to compete in the upstream content market.[33] For example, an unaffiliated content provider might be denied the same QoS as that offered to an affiliated provider, or an unaffiliated content provider might be offered the same QoS at a higher price than that offered to an affiliated content provider.[34] Net neutrality proponents also argue that surcharges for enhanced QoS would deter entry among upstart content providers by reducing expected profits.[35] We analyze those anticompetitive claims in Part II.C.

Finally, net neutrality proponents argue that the mere offering of enhanced QoS to any content provider (affiliated or not) implicitly or explicitly degrades the effective QoS received by all other content providers.[36] This position, of course, could be correct only to the extent

32. Quinn, *supra* note 20, at 8.

33. *See, e.g.*, Lawrence Lessig & Robert W. McChesney, *No Tolls on the Internet*, WASH. POST, June 8, 2006, at A23.

34. It generally does not matter to net neutrality proponents whether the affiliated provider offers content that competes with the unaffiliated content. They argue that QoS preference for any traffic necessarily discriminates against all other traffic.

35. Ben Klemens, *Net Neutrality Fosters Competition Between Technologies*, SCRIPPS HOWARD NEWS SERVICE, Aug. 17, 2006, http://www.shns.com/shns/g_index2.cfm?action=detail&pk=NET-NEUTRALITY-08-17-06.

36. *Net Neutrality: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 8 (2006) (statement of Lawrence Lessig, Professor of Law, Stanford University) ("Thus, working with the network provider, large video companies could secure sufficient provisioning to enable their content to be served while leaving insufficient

that overall broadband network capacities are constant and no content application ever tries to absorb more than its fair share of capacity—both counterfactual assumptions. Broadband access network capacities have been growing rapidly over the past several years,[37] and many popular applications seek to absorb all available access bandwidth.[38] Thus, the analogy of unaffiliated content providers being relegated to the "digital equivalent of a winding dirt road"[39] is hyperbole. Such providers likely will continue to have more and more access to bandwidth available to them year after year. And for the same reason as painting a stripe down the middle of a road to create two lanes is likely to speed all traffic (no driver is permitted to hog both lanes by driving down the middle), offering enhanced QoS to some content providers at a surcharge may even benefit content providers that decline the option.

Against these alleged costs, one must weigh the social benefits associated with permitting access providers to offer enhanced QoS to content providers at a positive price.[40] Net neutrality proponents speak of enhanced QoS as if it were a hypothetical offering that would be employed by an access provider for anticompetitive reasons only. In reality, enhanced QoS offerings at certain layers of the networks for both end-users (primarily enterprise customers) and content providers are already prevalent in the marketplace, presumably because some (but not all) customers value those services. Access providers are considering extending QoS offerings more broadly through their networks.[41] Because these QoS offerings at service application layers of the network have

---

bandwidth to other competitors.").

37. *Cable Broadband Prices Stable; Video Rates Increase*, COMM. DAILY, Oct. 2, 2006 ("Transmission speeds rose at major operators. Cablevision raised download speeds 50% for Optimum Online customers this year to 15 Mbps and doubled upload speeds to 2 Mbps maximum . . . . Prices haven't risen in 3 years, said a Cablevision spokesman. Road Runner download speeds top out at 10 Mbps, compared with 1.5 Mbps in 1996, TW said. Comcast increased online speeds 4 times and added many features at no charge the past 3 years, said a spokeswoman.").

38. For a discussion of how Skype supernodes may saturate users' connections, *see* Juha Saarinen, *Skype Supernodes Sap Bandwith*, COMPUTERWORLD, Oct. 25, 2005, http://www.computerworld.co.nz/news.nsf/news/7AB67323D6305E49CC2570A1001698C0; Posting of Om Malik to GigaOM, http://gigaom.com/2006/01/10/skype-the-bandwidth-hog (Jan. 10, 2006).

39. Lessig & McChesney, *supra* note 33.

40. Other articles have examined the consumer welfare effects associated with net neutrality provisions. *See*, *e.g.*, J. Gregory Sidak, *A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet*, 2 J. COMPETITION L. & ECON. 349 (2006), *available at* http://jcle.oxfordjournals.org/cgi/reprint/2/3/349; LARRY DARBY, AM. CONSUMER INST., CONSUMER WELFARE, CAPITAL FORMATION AND NET NEUTRALITY: PAYING FOR NEXT GENERATION BROADBAND NETWORKS (2006), *available at* http://www.theamericanconsumer.org/Net%20Neutrality%20Study.pdf.

41. Net neutrality proponents generally have not attacked current QoS offerings, but they express immense concern for any expansion of QoS.

been good for content providers and their subscribers, expansions of these QoS offerings to other layers of network may also be beneficial.

In Part II, we survey some of the current tiered QoS offerings in the marketplace. Some of the most compelling QoS offerings in the market are caching and prioritization services for content providers that supply "QoS-needy" content, such as online multiplayer video game providers. These enhanced QoS service offerings are not costless. As we shortly explain, access providers in fact incur costs for providing enhanced QoS. We also review findings in the economics literature that show how a network without QoS-type management would be prohibitively expensive for end-users. These two results combined—(1) positive costs of providing QoS and (2) consumer benefits associated with managed networks relative to unmanaged networks—provide a procompetitive, efficiency justification for offering enhanced QoS at a surcharge.

We also critique in Part II the anticompetitive hypothesis that is proffered by net neutrality proponents. In particular, we examine the incentives and the ability of an access provider to foreclose unaffiliated content providers by offering enhanced QoS at a surcharge. We conclude that an access provider that lacks monopoly power in the broadband access market—a condition that applies to the vast majority of all access providers in the United States—lacks any ability to foreclose unaffiliated content providers—and even if some of these access providers may enjoy some market power in some local markets, they still lack significant economic incentives to foreclose unaffiliated content providers.

In Part III, we explore how an access provider would respond if required to comply with the non-discrimination provisions in the proposed legislation. Under one scenario, an access provider would withdraw its enhanced QoS offerings, thereby depriving its customers of those options entirely. Under another scenario, an access provider would standardize its QoS offerings and embed the surcharge for "blended QoS" into the basic service price of a complementary offering such as hosting or access. We analyze some of the consumer welfare and innovation effects associated with both outcomes. We estimate that by 2009, the consumer surplus associated just with online multiplayer video games, which depend critically on QoS, will be between $729 million and $1.458 billion. The same analysis is broadly applicable across all other QoS-needy content—both existing content and content still under development. We also estimate the welfare effects of higher monthly broadband prices that would result from forcing access providers to meet the growing demand for Internet services without building intelligence into their networks. Using highly conservative estimates of the elasticity of demand for broadband, we calculate up to one-third of broadband subscribers might disconnect their broadband connections in response to cost increases for access providers (which get passed on to consumers in

the form of higher prices).

Finally, we explore the implications for U.S. broadband leadership that would result from net neutrality regulation. Proponents of net neutrality consider more regulation of access providers to be an elixir for all that ails the U.S. broadband industry, including the allegedly low broadband penetration rates or network capabilities in the United States. By increasing broadband access prices, however, net neutrality would undermine the particular objective of maximizing broadband penetration rates, and limiting the overlay of QoS capabilities seems unlikely to result in more capable networks. Of course, maximizing broadband penetration should not be the sole objective of policymakers. Future welfare depends on innovation by both access providers and content providers. By undermining the ability to contract for QoS, net neutrality would cause content providers to divert resources away from real-time applications or other QoS-needy applications. And by limiting the deployment of intelligent network engineering and preventing the tapping of ancillary revenue streams by access providers, net neutrality would undermine an access provider's incentives to expand and enhance their networks. As a result, the U.S. broadband industry would begin slouching towards mediocrity.

II. NET NEUTRALITY PROPONENTS ASSUME INCORRECTLY THAT ENHANCED QOS OFFERINGS CURRENTLY ARE HYPOTHETICAL AND WILL BE USED FOR ANTICOMPETITIVE REASONS ONLY

Net neutrality proponents speak of "access tiering"—that is, offering tiered levels of access or QoS at different prices—as if it is some hypothetical strategy that will be employed at some future date to foreclose unaffiliated content providers. In reality, tiered QoS offerings are already here at different layers of an access provider's network and for legitimate technical and economic reasons. Content providers are *voluntarily* entering into contracts with access providers presumably because content providers (and their customers) value these service enhancements more than the prices for these enhancements. Enhanced QoS is not forced upon content providers as part of some bundle of services that the providers otherwise do not want, or because the access provider has monopoly power over the supply of one of the products in the bundle. Furthermore, access providers offer enhanced QoS at a surcharge to content providers, not because they are trying to foreclose potential rivals in an upstream market or to degrade the quality for content providers that decline the QoS option, but because it is costly to offer such enhancements and because a managed network ultimately generates benefits for Internet users.

A. Enhanced QoS Offerings are Prevalent in the Marketplace Because They are Valuable to Some (But Not All) Consumers

There are two types of customers who are already purchasing enhanced QoS offerings: end-users (primarily enterprise customers) and content providers. For some subset of customers, enhanced QoS is valuable. For others, it is not. It necessarily follows that it makes little economic sense to force all customers to acquire the same level of QoS at the same price. In this section, we provide a handful of examples of enhanced QoS offerings for end-users and content providers in the marketplace today. This discussion is by no means exhaustive. Rather, it is intended to provide an overview for a non-technical audience.

1. Examples of Tiered QoS Offerings for End-Users

Not all end-users demand enhanced QoS. Typically, this option is sought only by businesses that have special communications needs. For example, medium and large businesses or "enterprise customers" want intranet (to allow employees to gain access to secured corporate information), extranet (to support business-to-business communications), and remote access (to provide traveling workers the same level of connectivity as individuals who work in branch offices). Enterprise customers can receive these services from an access provider through a private data network or a virtual private network, which provides the attributes of a private data network within a shared network infrastructure. A VPN allows a company to communicate confidentially over a publicly accessible network at a price significantly less than that of a comparable wide area network ("WAN"). VPN traffic can be carried over the Internet on top of standard protocols (such as IPsec) or over an access provider's private network with a defined Service Level Agreement between the customer and the service provider. A VPN customer can obtain enhanced QoS as a VPN option or as part of a defined SLA. Because Internet traffic traverses inside a customer's VPN on the access provider's network, that traffic gets preferential treatment vis-à-vis standard Internet traffic.

Most access providers offer VPN with a QoS option. For example, Verizon markets a VPN service called "IP VPN Dedicated" that allows a customer to send data across its global IP infrastructure with the security of a private network.[42] In conjunction with this service, Verizon offers a "Traffic Shaping/ Bandwidth Allocation" option that "helps provide real-time prioritization of outbound data from your LAN to the edge of our IP

42. Verizon Business, IP VPN Dedicated, http://www.verizonbusiness.com/us/data/dedicated (last visited Sept. 7, 2006).

network."[43] Verizon also offers SLAs for all access types and optional resiliency features.[44] AT&T markets two types of IP VPNs: network-based VPN and premises-based VPN.[45] On its website, AT&T explains that network-based VPNs use "advanced IP routing technology establishing and prioritizing route assignments."[46] AT&T also offers QoS and Class of Service ("CoS") traffic engineering capabilities for a customer's applications.[47] Qwest offers IP VPN under the name "Private Routed Network."[48] In conjunction with its VPN service, Qwest provides "optional security solutions including intrusion detection services, vulnerability assessments and customized professional services at an additional cost."[49] As part of its denial of service ("DoS") protection, Qwest offers an inspection engine that "extracts state-related information required from all application layers from the security decision and interprets these packets into 'conversations' . . . and looks for any abnormal behavior in a conversation."[50]

2. Examples of Tiered QoS Offerings for Content Providers

As is the case for end-users, not all content providers demand enhanced QoS. This option is demanded only by those content providers that supply QoS-needy content. Real-time applications represent an important type of QoS-needy content. Real-time video, VoIP, and online video game traffic cannot be experienced properly by the end-user if it is subjected to jitter (unevenness in the rate of data packet delivery). Accordingly, real-time content providers demand enhanced QoS.

Access providers currently may offer enhanced QoS to content providers in the form of managed hosting, local caching of content in nearby data centers, and prioritization of traffic at the IP packet layer. By purchasing hosting services from an access provider, a content provider can gain immediate access to the access provider's network. A content provider can also take advantage of the access provider's SLAs, under which the access provider is required to provide proof of a promised level of service. Each SLA contains a technical component, which offers

---

43. *Id.*
44. *Id.*
45. AT&T, Network-Based VPN, http://www.business.att.com/service_fam_overview.jsp?repoid=ProductSub-Category&repoitem=eb_network-based_vpn&serv_port=eb_vpn&serv_fam=eb_network-based_vpn&segment=ent_biz (last visited Aug. 28, 2006).
46. *Id.*
47. *Id.*
48. Qwest, Private Routed Networks (VPN), http://www.qwest.com/pcat/large_business/product/1,1016,782_4_28,00.html (last visited Sept. 7, 2006).
49. *Id.*
50. *Id.*

several classes of service. A content provider can request that an access provider offer a fully managed hosting solution or it can manage its own applications hosted in an IDC owned by an access provider. For example, Qwest offers the following commitment to customers that outsource their web presence: "[y]ou receive industry-leading SLAs. Many data centers are built with high degrees of redundancy in critical systems such as power, HVAC, fire detection and suppression and security."[51]

Online video game providers may purchase enhanced QoS as an option with hosting services from access providers. For example, Sony produces *EverQuest*, a three-dimensional fantasy massively multiplayer online role-playing game ("MMORPG") that requires users to pay a recurring monthly fee.[52] For a time, *EverQuest* was the most popular MMORPG in the industry.[53] Blizzard Entertainment produces *World of Warcraft*, another MMORPG set in a fantasy environment. As of September 2006, *World of Warcraft* had almost seven million active subscriptions worldwide.[54] In both games, online subscribers control a character avatar "exploring the landscape, fighting monsters and performing quests on behalf of computer-controlled characters."[55] In addition to cash incentives for good performance, a player is rewarded with experience that allows her character to improve in skill and power.[56] MMORPG games have hundreds of thousands of users playing simultaneously. To achieve the best possible fantasy environment for their online gaming websites, Sony and Blizzard place their servers in Internet data centers ("IDCs") owned by access providers around the world. They simply cannot afford for the players of their games to experience jitter.

AT&T hosts many of the largest online games.[57] AT&T's hosting service spans 30 IDCs across four continents, including locations in Paris, Shanghai, California, and Singapore.[58] A content provider that purchases managed hosting service can obtain SLAs relating to (1)

---

51. Qwest, Qwest® Dedicated Hosting Services – Infrastructure, http://www.qwest.com/largebusiness/products/esolutions/hosting/hostingInf.html (last visited Sept. 7, 2006).

52. Wikipedia, EverQuest, http://en.wikipedia.org/wiki/Everquest (last visited Aug. 26, 2006).

53. *Id.*

54. Seth Schiesel, *Online Game, Made in U.S., Seizes the Globe*, N.Y. TIMES, Sept. 5, 2006, at A1.

55. Wikipedia, World of Warcraft, http://en.wikipedia.org/wiki/World_of_Warcraft (last visited Sept. 7, 2006).

56. *Id.*

57. *See* Podcast: AT&T Hosts Multiplayer Online Gaming (providing a podcast of an interview by Larry Meyer with Chris Costello, Director of Product Management for managed hosting at AT&T), *available at* http://www.att.com/gen/landing-pages?pid=7728.

58. *Id.*

network response time, (2) application response time, and (3) application performance.

As part of an enterprise hosting service, a content provider can place its content on the access provider's servers to reach end-users faster and more reliably than from the content provider's servers alone. For example, Verizon markets a service called "Application Acceleration" on its website, which offers content providers "a high-performance web application delivery platform so [their] distant end-users get the same level of performance [their] local users enjoy."[59] AT&T markets a similar service under the name "Intelligent Content Distribution Service."[60] It bears emphasis that this form of QoS (along with other forms) may be supplied by third parties in addition to access providers. For example, Akamai Technologies provides a similar content-acceleration service by caching content closer to the end-user for over 2,000 customers.[61] One measure of the size of the market for acceleration services is Akamai's revenues, which reached $100 million in the second quarter of 2006.[62] The fact that Akamai offers enhanced QoS at a surcharge to content providers suggests that the same conduct by an access provider is based on justifiable business practices that could be found in what net neutrality proponents believe are otherwise competitive markets.

Among its many types of customers, Akamai provides enhanced QoS to online gaming providers. In August 2001, Akamai announced that it would power the first Internet-based suspense thriller, *Majestic*, on the EA.com website.[63] Akamai described the critical role of QoS in the online gamer's experience as follows:

> Akamai is providing the on-demand streaming delivery services for the *Majestic* game, delivering audio and video transmissions of information integral to the *Majestic* story, while helping to enhance the game's interactive experience for players. *Majestic* places players

---

59. Verizon Business, Application Acceleration, http://www.verizonbusiness.com/us/itsolutions/acceleration (last visited Sept. 6, 2006).

60. AT&T, Intelligent Content Distribution Service, http://www.business.att.com/service_fam_overview.jsp?repoid=ProductSub-Category&repoitem=eb_intelligent_content_distribution&serv_port=eb_hosting_storage_and_it&serv_fam=eb_intelligent_content_distribution&segment=ent_biz (last visited Sept. 7, 2006).

61. Press Release, Akamai Technologies, Akamai Reports Second Quarter 2006 Results (July 26, 2006), *available at* http://www.akamai.com/html/about/press/releases/2006/press_072606.html [hereinafter *Akamai Second Quarter Results*].

62. *Id.*

63. Press Release, Akamai Technologies, Akamai Supports EA.com's Highly Interactive Internet Suspense Thriller, Majestic (Aug. 17, 2001), *available at* http://www.akamai.com/html/about/press/releases/2001/press_081701.html.

> in the center of an unfolding mystery adventure, and delivers a highly personalized experience through common everyday devices that are connected to the Internet through which to tell its story. A critical part of the *Majestic* experience comes when players explore for clues and information on the Internet using the *Majestic* search engine. As users experience the game, online newscasts, web-cam recordings and audio transmissions provide information relevant to the game while interactive streaming audio and video clips, delivered by Akamai, provide clues to help solve the mystery. With Akamai's streaming service, *Majestic* users receive reliable, high-quality broadband and narrowband experiences regardless of spikes in traffic via Akamai's globally distributed network of more than 11,600 servers located at the edge of the Internet.[64]

As Akamai makes clear, the user's experience depends heavily on streaming video and audio clips, which in turn rely on QoS. In Part III below, we rely on this evidence to model how consumers would be affected if QoS offerings were removed from the marketplace.

B. Because Enhanced QoS is Costly to Provide, and Because a Managed Network Produces Consumer Benefits, the Use of Tiered QoS Offerings is Motivated by Procompetitive Reasons

In this section, we explain why it is procompetitive for an access provider to impose a surcharge for enhanced QoS. Very simply, access with QoS or hosting with QoS is a *different* and more costly product from plain access or plain hosting. Hence, when an access provider imposes a surcharge for enhanced QoS, it is not technically engaging in price discrimination—that is, it is not offering the same product to two different customer classes (one with a high willingness to pay, one with a low willingness to pay) at two different prices.

1. Enhanced QoS is Costly to Provide

An access provider's marginal cost of carrying a given traffic stream is equal to the opportunity cost associated with allocating resources away from carrying another stream. According to Jon Peha, Professor of Electrical Engineering and Public Policy at Carnegie Mellon, "the cost per bit of a stream with strict QoS requirements is greater than the cost per bit when QoS requirements are lax."[65] Welfare considerations demand that access providers be entitled to recover any increase in marginal cost associated with supplying enhanced QoS through higher prices. In particular, under a standard "Ramsey pricing"

64. *Id.* (emphasis supplied.)
65. Peha, *supra* note 3, at 8.

formulation designed to maximize social welfare, the price of any service is proportional to the marginal cost of providing that service and inversely proportional to the elasticity of demand for that service.[66] Indeed, it would be inappropriate for the access provider not to impose a price for enhanced QoS, as such pricing would amount to a subsidy. Economists have long recognized that subsidies result in a misallocation of resources. Applied here, free QoS enhancements would encourage over-consumption of QoS-needy traffic relative to the socially optimal level (which occurs when the marginal cost of providing the last unit of QoS equals the price).

2. A Network without QoS Management Would be Prohibitively Expensive for End-Users

A network operator can expand capacity by either investing in traffic control or adding network capacity or both. Without any regulatory distortions, an access provider will invest in each input until the marginal revenue product from the last dollar invested in traffic control (scaled by the price of traffic control) equals the marginal revenue product from the last dollar invested in network capacity (scaled by the price of adding capacity). As this optimality condition makes clear, the outcome of this calculus will depend on the relative prices of processing (used for traffic control) and capacity. According to Peha, innovation in fiber-optics has decreased the cost of capacity, which has made investments in traffic control during the last decade less appealing.[67] But he cautions that "there are risks in embedding this conjecture [that the tradeoffs cut in favor of expanding capacity] into our laws and regulations."[68]

As high bandwidth, real-time services such as streaming music and video gain in popularity, access providers will be forced to upgrade their access and backbone networks. Richard Clarke, Director of Economic Analysis of AT&T, has estimated the cost per broadband subscriber of a new network that attempted to satisfy the demand for Internet traffic exclusively through bandwidth—that is, the cost per user of a new, unmanaged network.[69] He demonstrates that as Internet usage patterns

66. *See*, *e.g.*, JEAN-JACQUES LAFFONT & JEAN TIROLE, A THEORY OF INCENTIVES IN PROCUREMENT AND REGULATION 30-31 (1993).

67. *See* Peha, *supra* note 3, at 8.

68. *Id.* at 9.

69. Richard N. Clarke, Costs of Neutral/Unmanaged IP Networks (May 2006) (unpublished manuscript, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903433). Clarke uses a simple quantitative model of the cost of an unmanaged PON-based IP network. He uses input values for the costs of the different elements of the network, including total number of broadband lines at a wire center, number of wire centers in a cluster, total broadband lines modeled, PON

become more bandwidth-intensive and real-time oriented, an unmanaged network would be extremely expensive for the typical consumer. In particular, he estimates that to provide sufficient capacity to accommodate the current typical Internet usage pattern in an unmanaged network, the cost per customer could reach $47 per month.[70] To provide sufficient capacity to accommodate expected growth in traditional Internet data services as well as use of Internet connections for bandwidth-intensive applications equivalent to just two simultaneous standard definition television channels per home, Clarke estimates that the cost per customer of an unmanaged network could reach $140 per month for Internet service only (not including the cost for video content).[71] Finally, if customers use the equivalent of viewing two simultaneous high-definition television ("HDTV") channels, Clarke estimates that the cost per customer of an unmanaged network could reach $466 per month.[72] Because current IP interoffice facilities and backbone cores are sized to provide roughly 45 Kbps that each subscriber currently uses during the network busy period, the major cost driver (from $47 per month to $466 per month) is not in the last-mile access portion of the network, but in the wire center cluster and backbone portions of the network.[73] Clarke concludes that it would be unlikely that enough customers would be willing to pay the fees to support an unmanaged network, which would render such business models commercially nonviable.[74]

C. Because Unaffiliated Content Providers Could not be Foreclosed from the Upstream Content Markets, the Use of Tiered QoS Offerings is Unlikely to be Motivated by Anticompetitive Reasons

Traditional foreclosure theories in economics require that the firm in question has monopoly power in some relevant product market and that the complementary market (in this case, Internet content) is subject

---

capacity code, maximum fiber splits, fiber splits at drop terminal, average wire center to wire center distance, sharing factor for wire center-to-wire center runs, fibers per wire center-to-wire center route, network router capacity sizing factor, and fraction of traffic leaving cluster.

70. *Id.* at 20.

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.* at 22 ("While it is possible that some customers so value the possible extra freedom and diversity they may enjoy from obtaining services over an unmanaged network that they may choose to pay these lofty prices, these are daunting figures for most customers. Fewer than 5% of all households are willing to pay as much as $150 per month for a "triple play" bundle of local telephone, long distance telephone and video services that includes programming costs. Thus, it seems unlikely that unmanaged PONs with capacity adequate to stream unicast video services will gain commercial traction.") (citations omitted).

to economies of scale. Although the second condition could be satisfied here, the first condition is clearly inappropriate. Setting aside the exact foreclosure strategy contemplated here (offering enhanced QoS at a positive price), we consider whether an access provider has both the incentive and ability to foreclose an unaffiliated content provider.

1. Access Providers Lack the Incentive to Foreclose Unaffiliated Content Providers

An access provider that discriminates in the provision of QoS to content providers acts anticompetitively to the extent that such activity leads to a reduction in consumer welfare. The relevant antitrust caselaw can best be explained as embracing a test that bans a monopolist from engaging in discriminatory refusals to deal with rivals where no inefficiency would result from sharing and where denying access to rivals enhances monopoly power.[75] To an antitrust court, substantial market power or monopoly power, rather than just some market power, is required because a firm cannot extend its power into a complementary market unless it wields substantial market power in the primary market.[76]

With the possible exception of certain cases, such as when buyers purchase more than one unit of the tying product and the individual demand curve is downward sloping,[77] "Chicago school" economists have demonstrated that vertical restraints generally are not motivated by anticompetitive reasons.[78] There are some exceptions, however, to the Chicago school concept of "a single monopoly rent." As Dennis Carlton explained in an *Antitrust Law Journal* article in 2001, the monopolist can earn incremental profits in the complementary market if (1) the complementary market is subject to economies of scale and (2) there exists some class of consumers who demand the complementary good

75. *See* Einer Elhauge, *Defining Better Monopolization Standards*, 56 STAN. L. REV. 253, 295–98, 305–14 (2003).

76. To an economist, the distinction between market power and monopoly power may not be as critical. For example, in one theoretical model where in a hypothetical monopolist attempts to squeeze surplus in the tying market by bundling, the only requirement is a downward sloping demand curve, which does not necessarily require monopoly power. Rather than distinguishing market power from monopoly power, it is more productive to focus on how substantial the foreclosing effects (resulting from the conduct) are.

77. For example, if the firm-level demand for the good in question could be downward-sloping and each firm demands multiple units, then the monopolist cannot capture 100 percent of the consumer surplus. *See*, *e.g.*, Patrick Greenlee, David S. Reitman & David S. Sibley, *An Antitrust Analysis of Bundled Loyalty Discounts* (Econ. Analysis Group, Discussion Paper No. 04-13, 2006), *available at* http://ssrn.com/abstract=600799. Clearly, content providers do not purchase multiple units of hosting or Internet access from access providers.

78. *See* ROBERT H. BORK, THE ANTITRUST PARADOX 290-98 (1978) (providing a review of the Chicago school literature). For example, the Chicago school models assume constant returns to scale in the tied market and a single unit purchased of the tying good.

only.[79] Critical to this model, however, is the requirement that the firm be a monopolist in the tying market.[80]

Applied here, proponents of net neutrality typically suggest that the local access market is not competitively supplied and that as a result there is a threat that the access provider could foreclose the complementary content market.[81] But although access providers have *some* power to set price (that is, some market power), there is clear evidence from marketplace that access providers lack *significant* power over prices (that is, substantial market power or monopoly power). Consider, for example, that the price of DSL service from Verizon has decreased from $49.95 per month for 768 kbps download speed in 2001[82] to $19.99 per month for the same download speed in 2007.[83] The price of cable modem service, adjusted on a per Mbps basis, also has declined significantly over the same time period.[84] With such substantial price declines, it is not reasonable to conclude that access providers have significant power to control access prices. Accordingly, a hypothetical claim involving an access provider's discriminatory pricing of QoS would not likely withstand antitrust scrutiny.

Another indicator of substantial market power or monopoly power is the ability to exclude rivals. But evidence of entry makes clear that this market power test also fails. According to the latest broadband report issued by the Federal Communications Commission ("FCC"), cable modem providers, the most popular form of broadband access

79. *See* Dennis W. Carlton, *A General Analysis of Exclusionary Conduct and Refusal to Deal - Why Aspen and Kodak Are Misguided*, 68 ANTITRUST L.J. 659 , 664-65 (2001).

80. To explain his theory, Carlton used as an example the case of a monopoly resort owner. *Id*. at 667-68. Guests at the resort, who are required to purchase all meals at the resort, are fully exploited by the monopolist. But to the extent that the resort can hold unaffiliated restaurants on the island below some minimum viable scale (condition 1) by requiring that resort guests purchase all meals at the resort, those unaffiliated restaurants will be forced to exit, and the island natives who did not demand a hotel room (condition 2) will be subjected to a monopolist in the supply of meals. Notice how Carlton's model requires that the firm be a monopolist in the resort market, else the resort would not be able to hold unaffiliated restaurants below some minimum viable scale because resort-goers who wanted to eat at those restaurants could simply go and stay at another resort without the limitation.

81. *See* H.R. 5273, 109th Cong. § 2.8 (2006) ("The overwhelming majority of residential consumers take broadband service from one of only two wireline providers, namely, from the cable operator or the local telephone company.").

82. Tom Spring, *Verizon Joins Broadband Price Hike Parade*, PCWORLD.COM, May 2, 2001, http://www.pcworld.com/resource/article/0,aid,48945,00.asp.

83. Verizon High Speed Internet, Plans, http://www22.verizon.com/ForHomeDSL/channels/dsl/packages/default.asp (last visited Feb. 15, 2007).

84. Jim Hu, *Comcast to Raise Broadband Speed*, CNET NEWS.COM, Jan. 16, 2005, http://news.com.com/2100-1034_3-5537306.html. Comcast cable modem customers with download speeds of 3 Mbps experienced an increase to 4 Mbps for no additional charge. Comcast customers with download speeds of 4 Mbps experienced an increase to 6 Mbps for no additional charge.

technology, accounted for just 57.5 percent of all residential high-speed lines in the United States as of December 2005, down from 63.2 percent in December 2003.[85] Although these data are gathered at the national level, they can be used to roughly characterize competition in a representative or average local broadband market.[86] The rapid decline in market share over a span of just two years implies that cable operators lack the ability to exclude rivals and thereby lack substantial market power. Cable providers lost share primarily to DSL providers, who upgraded their networks and slashed prices. Other broadband access methods are also growing, with satellite and wireless providers accounting for over half-a-million broadband connections according to the FCC's survey.[87] Moreover, new access technologies, such as Worldwide Interoperability for Microwave Access ("WiMAX") and broadband over powerline ("BPL"), emerged in the past few years to challenge incumbent broadband providers. WiMax technology began to develop in earnest in August 2006, when Sprint Nextel announced its plans to develop and deploy the first fourth generation ("4G") nationwide broadband mobile network, which will use the mobile WiMAX technology standard.[88] Working together with Intel, Motorola, and Samsung, "Sprint Nextel will develop a nationwide network infrastructure . . . that will support advanced wireless broadband services for computing, portable multimedia, interactive and other consumer electronic devices."[89] "The Sprint Nextel 4G mobility network will use the company's extensive 2.5GHz spectrum holdings, which cover 85 percent of the households in the top 100 U.S. markets . . . ."[90] Regarding BPL, the FCC counted over 5,000 BPL lines as of December 2005[91]—an impressive number, considering the technology's brief existence in the market.

Most importantly, proponents of net neutrality fail to grasp the nexus that compelling content drives the demand for broadband access. If real-time applications fail to emerge, then access providers will not be able to sell faster and more expensive (such as fiber-to-the-home)

85. WIRELINE COMPETITION BUREAU, FED. COMMC'NS COMM'N, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF DECEMBER 31, 2005 tbl.2 (2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266596A1.pdf [hereinafter *FCC High-Speed Services*].

86. Of course, there are some local markets that are served by only one broadband provider, in which case national shares are not a good measure of the degree of competition.

87. *FCC High-Speed Services*, *supra* note 85, at tbl.3.

88. Press Release, Sprint Nextel, Sprint Nextel Announces 4G Wireless Broadband Initiative with Intel, Motorola and Samsung (Aug. 8, 2006), *available at* http://www2.sprint.com/mr/news_dtl.do?id=12960.

89. *Id.*

90. *Id.*

91. *FCC High-Speed Services*, *supra* note 85, at tbl.6.

connections to end-users. And as we demonstrate below, even if access providers were somehow convinced that their profits could be increased through foreclosure, access providers lack the ability to induce unaffiliated content providers to exit the industry or to operate at a less efficient scale.

2. Access Providers Lack the Ability to Foreclose Unaffiliated Content Providers

Even if they wanted to, access providers cannot easily monopolize, let alone effectively compete in, content markets. In this section, we focus on the most likely content markets that access providers might attempt to monopolize—namely, content markets that are currently profitable to serve. Perhaps the most important submarket among the profitable Internet content markets is the market for advertiser-supported search engines. Other profitable submarkets include online payment systems, online games, and video-sharing websites. It bears emphasis that broadband access providers generally have not attempted to enter any of these three Internet content submarkets. The current industry leaders for search engines include Google, Yahoo!, Microsoft ("MSN.com"), and IAC/Interactive ("Ask.com"). Google offers advertisers AdWords, which places advertising links next to relevant search results and charging for clicks and for keywords. Google also offers AdSense, a system that places "sponsored" links on the web pages of newspapers and other publishers that sign up to be part of Google's network. "AdWords and AdSense produced $6.1 billion in revenues for Google [in 2005]."[92] Yahoo! entered this submarket by purchasing Overture in 2003 for $1.6 billion.[93] Microsoft built adCenter, which serves as the advertising system for searches on MSN.[94] As of June 2006, *The Economist* estimated Google's market share in search at roughly 50 percent.[95] Online search is characterized by high barriers to entry: "[b]ut because barriers to entry in the search business are high—the engineering talent is limited and data centres that can simultaneously support millions of searches are expensive—most analysts think that the four big search engines will stay ahead of the tiny ones."[96] The fact that America Online ("AOL"), once a leader in dial-up Internet access, permanently outsourced its search technology to Google indicates that barriers to entry in search can impede even established and well-funded

92. *The Ultimate Marketing Machine*, ECONOMIST, July 8, 2006, at 61-62.
93. *Id.*
94. *Id.*
95. *The Un-Google,* ECONOMIST, June 17, 2006, at 65.
96. *Id.*

Internet firms.[97] Likewise, Google's stock price as of March 2007 in excess of $450 per share (and resulting market capitalization in excess of $140 billion) implies that the barriers to entry to search engines are not easily surmountable.[98] These barriers to entry would extend to all potential entrants in the search submarket, including access providers.

In addition to the high entry barriers in the content markets, local access providers have no leverage over national (and in many cases, international) content providers, further undermining the prospect of an access provider monopolizing the content markets. At least one of the authors has been cited for support of the proposition that Internet content providers are vulnerable to vertical foreclosure strategies in the net neutrality debate.[99] But this application of the theory of vertical foreclosure assumes incorrectly that a content provider is offering content that is particular to a given locality and therefore requires access to a single broadband provider's subscribers. The vast majority of Internet content appeals to all U.S. residents, not just the residents of a particular locality. Thus, the relevant geographic market for assessing hypothetical foreclosure strategies in broadband is conservatively the United States, and more realistically, the world. Because Comcast, *the largest broadband service provider in the United States*, controls access to only 23 percent of all broadband subscribers, Comcast lacks the ability to induce a content provider from exiting the industry or even operating at an inefficient scale.[100] The next largest providers are AT&T and Verizon, each with roughly 14 percent of the U.S. market.[101]

Moreover, the unique relationship between an unaffiliated Internet content provider and an access provider is not conducive to foreclosure

---

97. *AOL to Use Google Searches*, WASH. POST, May 2, 2002, at E2.

98. Yahoo! Finance, GOOG: Summary for Google,,http://finance.yahoo.com/q?s=GOOG (last visited Mar. 26, 2007).

99. *See, e.g.*, Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. ON TELECOMM. & HIGH TECH. L. 329, 334 n.13 (2007) (citing Daniel L. Rubinfeld & Hal J. Singer, *Vertical Foreclosure in Broadband Access?*, 49 J. INDUS. ECON. 299 (2001)).

100. WIRELINE COMPETITION BUREAU, FED. COMMC'NS COMM'N, HIGH-SPEED SERVICES FOR INTERNET ACCESS: STATUS AS OF JUNE 30, 2006 tbl.2 (2007) (providing total broadband subscribers), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-270128A1.pdf; RICHARD A. BILOTTI ET AL., MORGAN STANLEY RESEARCH, CABLE/SATELLITE: LOOKING INTO 3Q06 AND 2007: CAUTIOUS ON TOP LINE, CAPITAL EXPENDITURES, AND LOFTY VALUATIONS (2006) (providing Comcast's subscribers for year end 2006).

101. Press Release, Verizon Investor Relations, Verizon's 4Q 2006 Results Cap Strong Year of Organic Growth in Wireless, Broadband and Business Markets (Jan. 29, 2007), *available at* http://investor.verizon.com/news/view.aspx?NewsID=813; AT&T INVESTOR BRIEFING, AT&T POSTS STRONG THIRD-QUARTER EARNINGS GROWTH; RESULTS DRIVEN BY WIRELESS REVENUE GAINS AND MARGIN EXPANSION, MERGER INTEGRATION PROCESS, IMPROVED BUSINESS TRENDS 16 (2006), *available at* http://www.att.com/Investor/Financial/Earning_Info/docs/3Q_06_IB_FINAL.pdf.

strategies. With a few exceptions (such as ESPN360), Internet content is not acquired by access providers at a certain cost per subscriber per month, as is the case with traditional video programming. Setting aside the seldom used leased access rules, unaffiliated video content providers cannot reach a video distributor's customers *unless the distributor has acquired the content from that content provider*. By contrast, unaffiliated Internet content providers do not need to reach an agreement with a broadband access provider to reach that access provider's broadband customers. Hence, access providers and unaffiliated content providers are not likely to get into a carriage dispute arising over price or affiliation. Although such disputes are common in the video programming industry, and Congress has given the FCC powers to prevent discriminatory practices,[102] because Internet content providers do not depend on access providers to reach end-users in the same way that video programmers depend on cable or DBS providers, video programming is the wrong framework for analyzing discriminatory strategies in Internet content markets. Even if an access provider were to refuse to supply enhanced QoS to an unaffiliated content provider, the only content providers that could be affected would be real-time content providers. But even here, the refusal to supply enhanced QoS would have to be coordinated across multiple access providers to have any meaningful foreclosure effect. Internet content markets are inherently national in scope. Thus, a content provider does not depend on a single local access provider to achieve critical economies of scale. (Contrast this with localized content in traditional video markets, such as sports programming, that depends on a handful of downstream providers to reach critical scale.) Without such coordination among broadband access providers, the foreclosed content provider could still achieve its efficiencies from the customers of other access providers.

Given the barriers to entry in the Internet content market, the caliber of the firms that currently supply Internet content (which implies that foreclosure would be very costly), and the unique relationship between Internet content providers and access providers, it is difficult to conceive how an access provider could leverage its alleged power in broadband access into the content market by imposing a surcharge on content providers for enhanced QoS. The last time an Internet service provider ("ISP") with downstream market power (in this case, dial-up Internet access) tried to build a "walled garden" to leverage its customer base into the upstream content market it met with unmitigated disaster.[103] To be

102. *See* 47 U.S.C. § 536 (a) (2000).

103. Wikipedia, AOL, http://en.wikipedia.org/wiki/AOL (last visited Feb. 13, 2007) ("[AOL] has since attempted to reposition itself as a content provider similar to companies such as Yahoo! as opposed to an Internet service provider which delivered content only to

fair, AOL's attempt to extend it power into the content market was not helped by the ubiquitous deployment and adoption of broadband technologies, which rendered unaffiliated ISPs less valuable.[104] But even before the advent of broadband, AOL failed to extend its considerable market power in dial-up Internet access into content markets. There is no reason to expect a different outcome for broadband access providers. In summary, access providers lack the incentive and ability to foreclose unaffiliated content providers. Tiered QoS offerings cannot be motivated by anticompetitive reasons.

III. BY REQUIRING NON-DISCRIMINATION IN THE PROVISION OF QOS, NETWORK NEUTRALITY PROPOSALS WOULD DESTROY THE SOCIAL BENEFITS ASSOCIATED WITH CURRENT TIERED QOS OFFERINGS

In this section, we provide a non-technical discussion of how consumer welfare could be decreased by access providers' attempt to comply with the non-discrimination provisions of the net neutrality proposals. A technical analysis of the welfare reduction is provided in sections A and B. Readers who are not technically inclined can understand the mechanism by which consumers would be harmed in what immediately follows.

Consumers voluntarily purchase enhanced QoS because the value created through this feature exceeds the incremental price. The difference between a customer's willingness to pay for a feature and its price is called consumer surplus. Consumer welfare is the sum of the surplus across all consumers in the market. In this section, we examine the consumer welfare effects that would flow from an access provider's likely response if required to comply with the non-discrimination provisions in the net neutrality proposals. As explained earlier, online video games, streaming multimedia, VoIP, video teleconferencing, alarm signaling, and safety-critical applications such as remote surgery may require some level of QoS. For ease of exposition, we focus on the consumer welfare effects for one of the most popular QoS-needy applications—online gaming. The same analysis could be applied to any other QoS-needy application.

We consider the consumer welfare effects of an access provider's attempts to comply with the non-discrimination provisions relating to QoS under two scenarios. In the first scenario, access providers attempt to comply with the non-discrimination provision by (1) withdrawing their enhanced QoS offerings entirely and (2) relying entirely on

subscribers in what was termed a 'walled garden.'").

104. *See*, *e.g.*, Robert W. Crandall & Hal J. Singer, *Life Support for Unaffiliated ISPs?*, 28 REG. 46, 49 (2005).

bandwidth to accommodate the growth in demand for Internet traffic. This scenario assumes that an access provider could not embed the price of some "blended" QoS in a complementary product purchased by the content provider (the basis of the second scenario). By withdrawing enhanced QoS from the marketplace, many QoS-needy applications would not function properly, and thus the demand for those products (and the consumer welfare associated with enjoying those products) would disappear. In the extreme case, the demand for such applications would either disappear entirely or fail to develop. As explained above, the proposals define a broadband network provider so broadly that they could limit QoS offerings at positive prices by non-network QoS suppliers such as Akamai. Even if some non-network QoS suppliers were immune from the regulation, the demand for QoS-needy applications would still shift inwards to the extent that network suppliers can offer some level of QoS beyond that offered by non-network suppliers or the price of enhanced QoS would increase to monopoly levels or both.[105] The effect would be to largely eliminate any welfare that is currently enjoyed by customers of QoS-needy applications.

Next, by relying entirely on an unmanaged network, the monthly cost per subscriber would rise to levels that could not be sustained in the marketplace. If the cost per subscriber of an unmanaged network were to increase to $47 per month, then the monthly subscription fee would need to increase even further, thereby inducing a significant portion of broadband customers to disconnect from the Internet or seek less costly alternatives. Based on estimates of the elasticity of demand for broadband access, we attempt to estimate the percentage of existing broadband subscribers who would disconnect their services in response to such a price increase.

In the second scenario, we posit that access providers would attempt to comply with the non-discrimination provisions by offering a blended, one-size-fits-all QoS offering to all content providers. Because access providers could not explicitly charge for QoS, they would likely provide a blended level of QoS that came standard alongside a (slightly more expensive) purchase of Internet access or hosting products—that is, an access provider would embed the price of blended QoS in some complementary product. But a uniform level of QoS—even at a lower price—would harm QoS-needy content providers such as Sony and Blizzard by depriving them of the QoS needed to make their applications function properly. Even worse, a blended QoS would harm the vast majority of content providers that have no demand for QoS but would

105. With enhanced QoS capabilities at both the access level and the backbone level, however, an access provider could set its content distribution service apart from Akamai's offering.

now be forced to pay for it. The theoretical underpinnings of such a reaction (and the resulting reduction in consumer welfare) have been recently provided by Professors Michael Katz and Benjamin E. Hermalin of the University of California at Berkeley.[106] In particular, they examine the effects of product-line restrictions in a duopoly (a market supplied by two firms).[107] They demonstrate that a restriction of the number of products that each firm can offer (applied here, the levels of QoS that can be associated with access or hosting service) may lead firms to choose the same quality of service (high or low), or it may lead them to choose non-overlapping products (high and low) where they would otherwise have engaged in head-to-head competition across all product variants.[108] They show that the resulting loss of competition can harm both consumers and economic efficiency,[109] and provide the following intuition:

> [t]here are two mechanisms through which a single-product restriction harms welfare in our duopoly model. In the unrestricted equilibrium, both firms offer both products. In the restricted equilibrium, the firms sometimes offer identical products and sometimes offer vertically differentiated products. When the firms offer identical products, the single-product restriction reduces welfare by eliminating what would have been efficient variety. When the firms offer vertically differentiated products the loss of direct competition leads to inefficient reductions in consumption levels. Consequently, both consumer and total surplus fall.[110]

In summary, total surplus is higher when the two firms compete without a single-product restriction than under three plausible outcomes (each firm chooses high quality, each firm chooses low quality, or one firm chooses high and the other choose low) with a single-product restriction.

The section concludes with a non-technical discussion of the effect of a non-discrimination provision on a content provider's incentive to innovate and on an access provider's incentive to deploy next-generation broadband networks. We discuss the implications of such competitive responses on our nation's leadership in the broadband industry.

---

106. Benjamin E. Hermalin & Michael L. Katz, *The Economics of Product-Line Restrictions With an Application to the Network Neutrality Debate* (Inst. of Bus. & Econ. Research Competition Policy Center, Working Paper No. CPC06-059, 2006), *available at* http://repositories.cdlib.org/iber/cpc/CPC06-059/.

107. *Id.* at 24-28.

108. *Id.* at 28-33.

109. *Id.* at 33-34.

110. *Id.* at 35.

A. Consumer Welfare Effects: An Access Provider Would be Forced to Withdraw or Standardize Its Tiered QoS Offerings

We posit that an access provider would attempt to comply with a non-discrimination provision in the supply of QoS by either withdrawing its enhanced QoS offering from the marketplace or by replacing its tiered QoS offerings with a one-size-fits-all or "blended" QoS offering. Under either scenario, consumer welfare associated with the purchase of enhanced QoS would be largely eliminated. To make our analysis concrete, we consider the demand for enhanced QoS by content providers that supply online multiplayer video games. A similar analysis could be performed for other content providers.

1. Consumer Losses Associated with Withdrawal of Current Tiered QoS Offerings

The net neutrality proposals in Congress would effectively establish a market price of zero for enhanced QoS. To the extent that QoS can be considered a standalone product offering (that is, a complementary offering to hosting and access), one can analyze an access provider's decision to offer QoS under the standard shut-down decision in economics. According to the Markey bill, if an access provider gives priority or offers enhanced QoS "to data of a particular type, [then it must] prioritize or offer enhanced quality of service to all data of that type (regardless of the origin of such data) *without imposing a surcharge* or other consideration for such prioritization or quality of service."[111] Content providers that did not yet contract for QoS could demand free QoS from access providers. Although the provision would not nullify existing contracts for QoS between access providers and content providers, a content provider that previously contracted for QoS would likely demand to renegotiate its terms after learning that its rivals were getting the same QoS for free. The classic shut-down decision in economics is to withdraw from supplying a service if the price is less than the average variable cost of supplying that service.[112] As explained above, the average variable cost of providing QoS is the opportunity cost of carrying a given traffic stream and thus exceeds zero.[113] Hence, it is

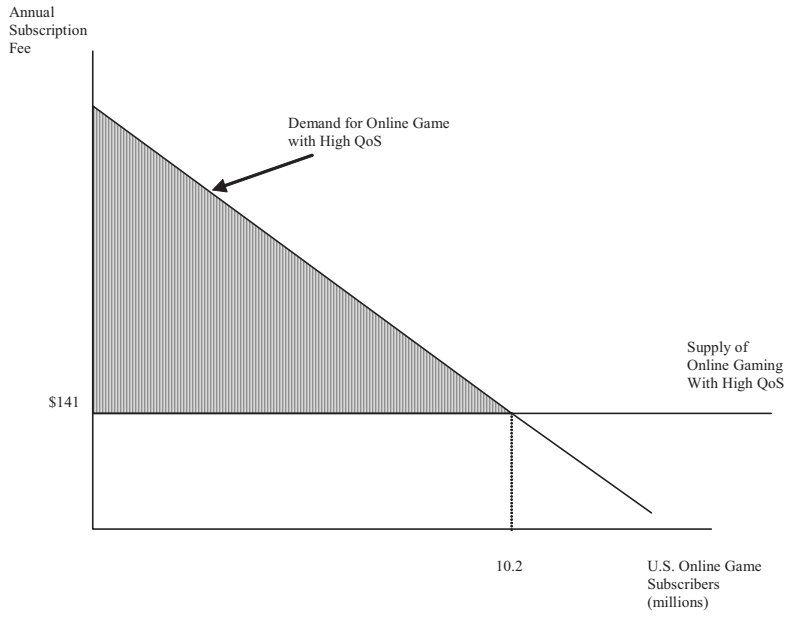
111. H.R. 5273, 109th Cong. § 4(a)(7) (2006) (emphasis added).

112. DENNIS W. CARLTON & JEFFREY M. PERLOFF, MODERN INDUSTRIAL ORGANIZATION 60 (1990).

113. These costs have been quantified. *See* Qiong Wang, Jon M. Peha & Marvin A. Sirbu, *Optimal Pricing for Integrated Services Networks*, *in* INTERNET ECONOMICS 353-76 (Joseph P. Bailey & Lee W. McKnight eds., 1997). *See also* Hermalin & Katz, *supra* note 106, at 19 ("Some participants in the network neutrality debate have argued that increased quality is essentially costless, at least up to some point. We doubt the empirical validity of this

reasonable to assume that an access provider would withdraw its QoS offering from the market entirely to comply with the non-discrimination provision.[114]

FIGURE 1: CONSUMER WELFARE LOSS OF ONLINE GAMERS ASSOCIATED WITH ELIMINATION OF ENHANCED QOS OFFERING



a. Elimination of Consumer Surplus Associated with the Purchase of Enhanced QoS

The consumer welfare eliminated under this "withdrawal" scenario is equal to the welfare currently enjoyed by consumers of enhanced QoS. To make our discussion concrete, we focus on the consumer welfare associated with the supply of enhanced QoS from content providers (obtained from access providers) to online gamers.[115] Clearly, the withdrawal of QoS enhancements by access providers will affect consumer surplus associated with other applications such as streaming video and music. Without QoS purchased by content providers like Sony and Blizzard, online gamers could not experience the game as it was

claim . . . .").

114. Even if these costs were entirely fixed, the access provider would not be able to recover its costs in the long run.

115. By online gamers, we refer to consumers of QoS-needy gaming content. For example, video poker would not constitute QoS-needy gaming content. By contrast, MMORPG or any other interactive or real-time gaming would be QoS-needy.

meant to be played. According to AT&T's Director of Product Management for Managed Hosting, "a couple of hundred milliseconds can make a big difference" in a user's experience during a MMORPG.[116] Figure 1 shows the demand curve for online games in 2006. The vertical access is the average annual subscription fee for online gamers (equal to the product of $11.75 per month and 12 months).

PriceWaterhouse Coopers projects 10.2 million online video game subscribers in the United States by the end of 2006.[117] Hence, annual industry revenue is equal to the product of 10.2 million subscribers and $141 per year, which is depicted graphically as the rectangular area under the supply curve. The number of online subscribers is expected to increase to 28.5 million by 2009.[118] With an average monthly subscription fee of $11.75 in 2006, the annual subscription spending in the United States in 2006 was estimated to be $1.438 billion (equal to $11.75 per month x 12 months x 10.2 million subscribers).[119]

To estimate the area under the demand curve, one needs an estimate of the elasticity of demand for online gaming. The elasticity of demand is equal to the percentage change in quantity demanded in response to a one-percent increase in the price of the good. The demand curve for a good with elastic (that is, more price-sensitive) demand is flatter than is the demand curve for a good with inelastic demand. Clements and Ohashi estimated the price elasticity of demand for entertainment software consoles between the years 1994 to 2002.[120] The average price elasticity across all consoles estimated by Clements and Ohashi was -2.58. We estimate the consumer welfare associated with the purchase of $1.4 billion in online games in 2006 under two scenarios. In the first scenario, we assume that the price elasticity of demand for online games is equal to Clements' and Ohashi's average price elasticity of demand across all gaming consoles (equal to -2.58). In the second scenario, we assume that the demand for online games is less elastic than the demand for consoles by a factor of two (equal to -1.29). The elasticity of demand for online gaming appears to be low, as recent price increases for online games have not reduced subscriptions.[121] Of course, the elasticity of demand will depend on the particular game. For example, the demand for

116. Podcast, *supra* note 57.

117. PRICEWATERHOUSECOOPERS LLP, GLOBAL ENTERTAINMENT AND MEDIA OUTLOOK: 2005-2009, 344 (2005). PriceWaterhouseCoopers defines online games as games that "enable players to compete against each other over the Internet." *Id.* at 343. Hence, this figure excludes any games that enable a user to play against a computer.

118. *Id.*

119. *Id.*

120. Matthew T. Clements & Hiroshi Ohashi, *Indirect Network Effects and the Product Cycle: Video Games in the U.S., 1994-2002* 29 (NET Inst., Working Paper No. 04-01, 2004).

121. *Console Wars: A Rare Bright Spot in the Gloomy Technology Industry, Video Games Are Growing Up*, ECONOMIST, June 20, 2002, at 1.

a cult favorite such as *World of Warcraft* may be less price elastic than the demand for the average online game.

Our estimate of the surplus associated with consuming online video games in the United States is $195 million for 2006—that is, consumers of video games were willing to spend roughly $195 million more than the price of online games. When one assumes that the elasticity of demand for online games is less elastic, our consumer welfare estimate increases to $250 million. Similar calculations can be performed for 2009, when the number of online subscribers is expected to increase to 28.5 million and the average monthly subscription fee is expected to decline slightly to $11. By 2009, the consumer surplus associated with online gaming will be between $729 million and $1.458 billion. The withdrawal of QoS offerings by access providers could jeopardize the consumer surplus associated with online gaming for every year in which net neutrality regulations are in force.

The same analysis could be used to calculate the destruction in consumer surplus associated with any real-time application. For example, in a VoIP application, which requires low jitter and delay, the packets must be received within 50 milliseconds.[122] Best efforts delivery, which does not ensure that packets travel in the same path and arrive serially at even intervals, could lead to unacceptable QoS for a VoIP. Although VoIP is currently acceptable to some users without QoS, in a network flooded with increased traffic from streaming video and HDTV, it is conceivable that VoIP would no longer be acceptable without QoS. To the extent that the demand curve for VoIP would shift inward as a result of unacceptable QoS, the consumer surplus associated with VoIP would be eliminated as well.

Finally, it is not clear whether the net neutrality bills would prevent access providers from offering any enhanced QoS to end-users at positive prices. For example, under the Snowe-Dorgan bill, access providers could offer prioritization (a form of QoS) to end-users but could not impose a fee for such service.[123] To the extent that access providers withdrew such offerings for end-users to comply with that provision, one would have to include the consumer welfare loss associated with the consumption of VPNs and other end-users services that make use of QoS.

122. Peha, *supra* note 3, at 7. According to Peha, if packets for a VoIP application are not received in 50 milliseconds, they are "useless."

123. S. 2917, 109th Cong. § 12(a)(5) (2006).

b. More Expensive Internet Access Associated with Unmanaged IP Networks

As we demonstrated above, the cost per customer of providing basic Internet access (and thus the price) would increase significantly if access providers were prohibited from using intelligent traffic control, including QoS, to meet the demand for Internet traffic. According to Clarke, the monthly cost of providing broadband access on an unmanaged network would increase by roughly one third (from $35 to $47) just to accommodate the transition from current typical Internet usage to that displayed by today's "power" users.[124] If the cost per subscriber were to increase to $47, then the price for broadband access would likely exceed $47 to allow access providers to earn a positive margin. Unfortunately, the demand for broadband access may be sufficiently elastic that many broadband subscribers would cancel their services before paying in excess of $47 per month for broadband access. As evidence of this sensitivity to prices around $50 per month, note that U.S. residential high-speed lines nearly *doubled* from 17.3 million in December 2002 to 42.9 million in December 2005[125] as broadband rates fell below $50 per month. Using a conservative estimate of a monthly price of $47 (which would not allow any incremental margin) and an own-price elasticity of demand for broadband access of -1.0, which is at the low end of estimates from several empirical studies,[126] we estimate that 14.7 million (34.3 percent) broadband subscribers would cancel their services before paying $47 per month for broadband access. The associated loss in annual consumer welfare for these "marginal" broadband customers would be large (roughly $1 billion per year), and the loss in annual consumer welfare associated with higher prices for the remaining broadband customers would be even larger (roughly $4 billion per year in higher payments for broadband access). More realistic estimates of the elasticity of demand for broadband and of broadband prices (which would allow for some incremental margin in an unmanaged network) would result in even larger welfare losses.

---

124. Clarke, *supra* note 69, at 20.

125. *FCC High-Speed Services*, *supra* note 85, at tbl.3.

126. *See*, *e.g.*, Hal R. Varian, *The Demand for Bandwidth: Evidence from the INDEX Project*, *in* BROADBAND: SHOULD WE REGULATE HIGH-SPEED INTERNET ACCESS? 57-83 (Robert W. Crandall & James H. Alleman eds., 2002) (estimating an elasticity of demand between -3.1 and -2.0); Austan Goolsbee, *The Value of Broadband and the Loss of Taxing New Technology*, 5 B.E. J. ECON. ANALYSIS & POL'Y 1505 (2006) (estimating a demand elasticity between -3.07 and -2.44); Robert W. Crandall, J. Gregory Sidak, & Hal J. Singer, *The Empirical Case Against Asymmetric Regulation of Broadband Internet Access*, 17 BERKELEY TECH. L.J. 953, 954 (2002) (estimating an elasticity of demand of -1.2); Gerald R. Faulhaber & Christiaan Hogendorn, *The Market Structure of Broadband Telecommunications*, 48 J. INDUS. ECON. 305, 326 (2000) (estimating an elasticity of demand of -1.533).

2. Consumer Losses Associated with Standardized QoS Offerings

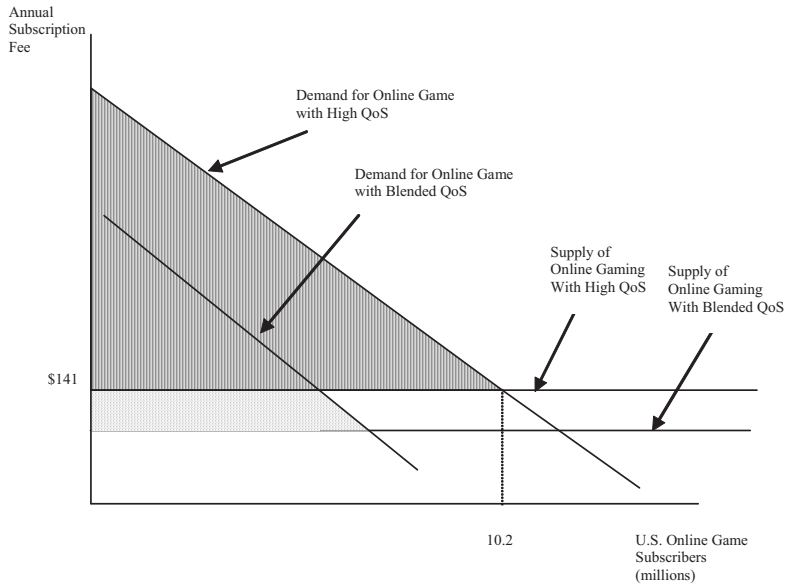
In this scenario, we posit that access providers, in an effort to comply with the non-discrimination provisions relating to QoS, embed a "blended" level of QoS as part of their standard hosting or access service for content providers. The blended level of QoS would likely be an average QoS that is superior to the QoS associated with plain hosting or access service but inferior to the QoS associated the current QoS options. Nothing in the net neutrality bills prohibits an access provider from charging more for complementary services such as access or hosting.

a. Content Providers and Their Customers Who Value Enhanced QoS Will be Forced to Settle for Something Less

The analysis of the loss in consumer welfare from a reduction in QoS is similar to the preceding analysis of the loss in consumer welfare from the elimination in QoS. Both scenarios result in an inward shift of the demand curve. Under this scenario, we posit that the demand for online games with blended QoS sits to the left of (or below) the demand for online games with enhanced QoS. Temporarily holding the supply curve constant, the effect of such a shift would be a reduction in consumer welfare, as the area of the triangle is reduced. The magnitude of the shift will depend on the extent to which online gamers are willing to tolerate a modest reduction in the quality of the game. This shift in the demand curve is depicted in Figure 2.

In addition to a shift in the demand curve, the supply curve of online video gaming could shift downwards. The supply curve can be thought of as the marginal cost of supplying online gaming. Under the status quo, online game producers such as Sony and Blizzard incur a marginal cost for acquiring a high level of QoS from access providers. Under the scenario contemplated here, however, content providers that previously acquired a high level of QoS would incur a lower marginal cost for acquiring a blended level of QoS, as *all* content providers—not just those that value QoS—would be required to share in the access provider's cost of providing blended QoS. Holding the demand curve constant, a downward shift in the supply of a product increases consumer welfare, as the size of the triangle increases. Because both the demand curve and the supply curve are affected by a reduction in QoS, one must balance the decrease in welfare from reduced demand (depicted by the vertical lines above the demand curve for blended QoS) against the increase in welfare from lower costs (depicted by the dotted area above the supply of online gaming with blended QoS).

FIGURE 2: CONSUMER WELFARE LOSS OF ONLINE GAMERS ASSOCIATED WITH BLENDED QOS OFFERING



Although the net welfare effect on online gamers is ambiguous in theory, it is reasonable to believe that the demand effect will likely exceed the supply effect, thereby resulting in a net reduction in welfare. With respect to the demand effect, online video gamers could be especially sensitive to even a slight degradation in the experience of the game. Most websites are free. To persuade a user to pay $25 per month for an online interactive game requires an exceptionally superior offering. For this reason, we expect the demand effect could be large. By contrast, it is not clear whether online game providers would pass on a large portion of the cost savings to their subscribers; only firms in perfectly competitive industries pass on 100 percent of the cost savings to consumers. Moreover, access providers would attempt to recover the cost of providing blended QoS service through higher prices of complementary products. Hence, the total cost of providing online gaming, including the cost of access and hosting services, will not decline as dramatically as the direct cost of QoS. For these reasons, we expect the supply effect could be small. On net, online gamers will likely be worse off, but by not as much as they would be if access providers were to withdraw QoS entirely (the first scenario).

b. Content Providers and Their Customers Who Do Not Value Enhanced QoS Will be Forced to Purchase Something They Do Not Value

Not all content providers value QoS. Indeed, as of September 2006, most websites did not produce QoS-needy applications. For example, real-time applications such as online gaming and VoIP are relatively recent offerings. (The 56 percent increase in Akamai's revenues from the second quarter 2005 to the second quarter 2006 implies that QoS-needy applications are growing and could one day represent a significant portion of total Internet traffic.[127]) In a world where every content provider must acquire some QoS, content providers who do not value those services will be unambiguously worse off. Because access providers could not charge explicitly for QoS under the current net neutrality bills, the fees would likely be imposed on complementary services purchased by content providers such as access and hosting.

To make this point concrete, consider a content provider that currently purchases hosting service from an access provider for $100 per month but declines the QoS option, which was priced at an additional $50 per month. Assume that ten percent of the access provider's customers chose the bundled hosting offering (hosting plus QoS) for $150 before the imposition of net neutrality. The average price per customer is thus $105 (equal to 0.9 x $100 + 0.1 x $150). Under a net neutrality regime, the price of the QoS option would be set to zero (by law) and the price of hosting service would increase to $105 if the access provider sought to preserve the average revenue per customer. Hence, the content provider that originally opted against QoS now incurs an additional charge of $5 per month for blended QoS. Faced with this higher incremental cost, the content provider would likely try to pass on a portion of this cost increase to its customers.

In summary, blended QoS would likely harm end-users of content providers that require enhanced QoS (by reducing the quality of QoS-needy applications), and it would unambiguously harm end-users of content provider that do not value QoS (by increasing the price of an unnecessary component). Indeed, it is hard to identify *any* constituency that would prefer a one-size-fits-all solution for QoS. (Indeed, this begs the question as to why Google and some other content providers are seeking such restrictions. We believe the most plausible explanation is that Google's most lucrative application—namely, online search—does not depend on high QoS to perform properly. As a result, Google would prefer to erect barriers to entry in QoS-needy content submarkets, even if

127. *Akamai Second Quarter Results, supra* note 61.

those barriers applied to itself.[128]) One class of content providers that could be better off would have a willingness to pay for enhanced QoS just below the current price for QoS. To use the simple example above, assume this particular content provider values high QoS at $45 per month (slightly below the market price of $50) but values blended QoS at $15 per month (slightly more than the incremental cost of the blended offering). Hence, under the blended QoS offering, this content provider earns incremental surplus of $10 (equal to $15 less $5). Public policy should not favor one class of content providers over the content providers at the ends of the distribution that either do not value QoS at all or value QoS highly.

B. Innovation Effects: Content Providers Will Divert Resources Away from QoS-Needy Applications and Towards Non-QoS-Needy Applications

How would a content provider that was developing QoS-needy content react to an access provider's attempts to comply with the non-discrimination provisions relating to QoS? Under either reaction posited above, withdrawal or blended QoS, high QoS would no longer be available to content providers that were developing QoS-needy applications. Hence, the net neutrality bills would effectively eliminate a market. Content providers interested in designing and producing QoS-needy content would have no means of providing that content, at least not in an acceptable manner. Accordingly, they will divert their resources and creative energies to other applications that do not require high QoS.

The analysis above, describing the reduction in consumer surplus flowing from a reduction in demand for QoS-needy applications, is broadly applicable across not just presently existing content, but also content still under development. Consider current efforts by Apple to deliver streaming video for Internet users. On September 13, 2006, Apple announced a device due in early 2007 called iTV that will display movies, television shows, and other videos purchased over the Internet on television sets.[129] The iTV device will connect directly to a user's television set, and it will access audio and video files stored on a user's computer through a common Wi-Fi.[130] Movies will take 30 minutes to download from Apple's iTunes Store.[131] Although current video clips

128. For other possible explanations for Google's seemingly non-self-serving strategy, including a coordinated refusal to deal among content providers, *see* Sidak, *supra* note 40, at 456-58.

129. Nick Wingfield & Merissa Marr, *Apple Computer Aims to Take Over Your Living-Room TV*, WALL ST. J., Sept. 13, 2006, at B1.

130. *Id.*

131. *Id.*

may not require high QoS (guaranteed throughput may be required for streaming video), as online video takes on a more interactive nature, it is not much of a stretch to envision how Apple or some other video provider would demand high QoS from access providers. By eliminating the market for QoS-needy applications entirely, net neutrality legislation would reduce consumer surplus not just for current QoS-needy applications, like online gaming, but also for applications not yet existing and that will never be developed in a world where there is no mechanism to deliver the relevant QoS-needy content.

C. Implications for U.S. Broadband Leadership

Proponents of net neutrality argue that imposing non-discrimination requirements in the provision of QoS will increase broadband penetration rates in the United States, thereby making the U.S. more competitive with other countries.[132] In particular, they argue that "robust competition in other nations' networks have made the debate over nondiscrimination (or Network Neutrality) moot in these countries," and that "any temptations to distort the content market are undercut by competition between multiple broadband providers."[133] They point out that, presumably as a result of deregulatory policies at the federal level, the United States has fallen to 16th place in the International Telecommunications Union's ("ITU") broadband penetration rankings and has fallen to 12th place in the penetration measures from the Organization for Economic Cooperation and Development ("OECD").[134]

Importantly, the authors note a strong correlation between broadband penetration rates and broadband prices.[135] Based on this result, they suggest that mandatory unbundling at cost-based prices would reduce prices and thereby stimulate broadband penetration:

> [t]he best broadband offerings in many of the countries shown above do not come from the traditional telecom incumbents, but from competitors who have entered historically monopolistic markets. This new competition was made possible by good public policy—specifically the successful implementation of 'open-access' or 'unbundling' requirements.[136]

Empirical research demonstrates that open access policies, after properly

132. *See, e.g.*, S. DERRICK TUCKER, FREE PRESS, CONSUMERS UNION & CONSUMER FED'N OF AM., BROADBAND REALITY CHECK II 5 (2006), *available at* http://www.freepress.net/docs/bbrc2-final.pdf.

133. *Id.* at 16.

134. *Id.* at 8.

135. *Id.* at 17.

136. *Id.* at 17.

controlling for other factors that influence broadband penetration, do not positively contribute to broadband penetration in a significant way.[137] In a cross-sectional regression of broadband penetration on several unbundling variables, Scott Wallsten of the AEI-Brookings Joint Center found that (1) the incremental effect of local loop unbundling ("LLU") on penetration is ambiguous, (2) the incremental effect of bitstream access on penetration is positive, but is not always statistically significant, and (3) the incremental effect of subloop unbundling on penetration is negative and statistically significant under all specifications.[138] Instead, Wallsten finds that population density (it is easier to connect broadband users if they live closer together), GDP per capita, country-specific factors, and time factors are more important in explaining variations in broadband penetration.[139] To the extent that mandatory unbundling fails to lower broadband prices—perhaps resellers fails to pass on to consumers any of the difference between the retail price and the regulated access price—mandatory unbundling cannot increase broadband penetration.

Because the demand for broadband access is sensitive to the price of broadband access, broadband prices are critical in driving broadband penetration. The relevant question, however, is how net neutrality provisions would affect the price for broadband access. Setting aside the issue of whether competition for U.S. broadband customers is sufficiently intense so as to render the issue "moot," proponents of net neutrality fail to provide the link between "temptations to distort the content market" with tiered QoS offerings and higher access prices. For at least two reasons, we believe that net neutrality legislation would *increase* the price of broadband access, and thereby decrease broadband penetration in the United States. First, the cost per customer of an unmanaged network would be prohibitively expensive. Clarke estimates that to the extent that consumer demand for more bandwidth-intensive applications continues to rise, the cost per customer of an unmanaged network will increase dramatically. These cost increases would be passed onto consumers in the form of higher broadband access prices. Second, access providers could use incremental revenues from content providers to partially subsidize the price of access for end-users.[140] Google, a wireless broadband access provider, is using this pricing strategy in Mountain View, California.[141]

---

137. Scott J. Wallsten, *Broadband and Unbundling Regulations in OECD Countries* 1 (AEI-Brookings Joint Ctr. for Regulatory Studies, Working Paper No. 06-16, 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=906865.

138. *Id.*

139. *Id.* at tbls.1, 2.

140. *See* Sidak, *supra* note 40.

141. John Markoff, *Google Says It Has No Plans for National Wi-Fi Service*, N.Y.

Finally, it bears emphasis that broadband penetration rates (while important) should not be the *sole* consideration in shaping broadband policy in the United States. If the objective of the U.S. government were exclusively to maximize broadband penetration, as opposed to maximizing static and dynamic efficiency, then the "optimal" policy would be to mandate unbundling to competitors at $0 per month, which would be tantamount to nationalizing all broadband infrastructure in the United States. Clearly, such a policy would be blatantly inconsistent with maximizing static and dynamic efficiency. In addition to broadband penetration rates, U.S. competitiveness in broadband services will ultimately depend on innovation by both access providers and content providers. Net neutrality would undermine the incentive of access providers and content providers to invest in new technologies. By limiting ancillary revenue streams for access providers, net neutrality would undermine an access provider's incentives to expand and enhance their networks. By mandating non-discrimination in the supply of QoS, content providers will be less inclined to take risks on QoS-needy applications. The rest of the world looks to the United States for creative content. Net neutrality would force them to look elsewhere.

TIMES, Aug. 16, 2006, at C7.

THE ANALOG HOLE AND THE PRICE OF MUSIC: AN EMPIRICAL STUDY

DOUGLAS C. SICKER,* PAUL OHM,** & SHANNON GUNAJI***

We present the results of surveys of music consumers exploring their willingness to pay for digital downloads of music and measuring the impact of the so-called analog hole. The analog hole refers to a perhaps-unavoidable vulnerability of most digital rights management systems. In short, because people cannot consume digital information directly, they must rely on devices to convert digital information into analog signals, which are very difficult to keep from being copied.

Although content providers decry the analog hole as a loophole of the technical measures they use to protect content, surprisingly little is known about its fundamental aspects. Can average users exploit the analog hole, or is this limited to sophisticated users? Does analog hole copying significantly degrade the quality of music or video? Will people pay for music that isn't a perfect digital copy? Intuitions and guesses abound, but until this article, no study has answered these questions. While the surveys' sample sizes were too small to form statistically significant conclusions, we discovered several interesting results including one tantalizingly specific result: what's the analog hole worth? Based on our survey, 24¢. That's how much less our survey respondents would pay for a music track when a perfect digital copy was replaced by an analog hole copy. Although our results must be replicated on a larger scale, they suggest many conclusions that have never before been proved: people are willing to pay for less-than-perfect analog hole copies of songs; people will pay much more than half the price of a typically-priced digital music file for its degraded alternative; and even self-avowed "pirates" show a willingness to pay for digital music, albeit at prices well below today's market standard of 99¢ per song.

* Assistant Professor of Computer Science and Telecommunications, University of Colorado.

** Associate Professor of Law and Telecommunications, University of Colorado School of Law. I would like to thank the editors of the *Journal on Telecommunications & High Technology Law*, and in particular Darlene Kondo, Micah Schwalb, and Michael Beylkin for their superb assistance.

*** Graduate Student, Interdisciplinary Telecommunications, University of Colorado.

I. INTRODUCTION

The music industry has come to trust that digital rights management technology ("DRM"), backed by laws like the Digital Millennium Copyright Act ("DMCA"), will keep most people from making unauthorized, perfect digital copies of DRM-protected content. Its increased faith has led it to license its music to various online music stores, which has helped spawn a thriving market for pay-per-download music. Nevertheless, the music industry frets about what is known as the analog hole, which arises from the simple fact that digital music must be converted to an analog signal at some point if it is to be enjoyed. It is very difficult, if not impossible, to prevent people from capturing these analog signals, re-digitizing them, and distributing them on the Internet, stripped of DRM. To try to "plug" the analog hole, Congress has considered bills that would mandate strict controls over what device manufacturers can do with analog ports and information.[1] This approach seems premature because there is much we do not yet know about the analog hole.

An empirical study of the effect of the analog hole is warranted. For example, whether the analog hole poses the threat that some claim depends on how it impacts consumer preferences. It may be that analog hole copies, which tend to have a degraded signal quality, are so much less preferred by consumers than higher fidelity, digital versions, as not to act as a market substitute at all. It may also be the case that exploiting the analog hole is so prohibitively complex or costly that it is unlikely to occur with any regularity. We begin to answer these empirical questions.

In this paper, we describe a series of empirical studies we conducted that establish four important results. First, readily-available commercial technologies can be used to exploit the analog hole to obtain, copy, and distribute DRM-protected digital content. These technologies are not difficult to use and require no specific expertise or computer skill. Second, we conducted consumer surveys which demonstrate that consumers can perceive the difference between analog hole copies and digital originals. Third, we also used surveys to determine consumer willingness to pay. These surveys reveal that consumers are willing to accept degraded-quality analog hole copies at a discounted price despite diminished quality. Although this result may seem intuitive, as far as we know, we are the first to examine the question with rigor and to quantify the actual price-point where piracy might be avoided. Our econometric model suggests that people would be willing to pay 75¢ for an analog hole copy of a 99¢ digital track.

1. *See* Digital Transition Content Security Act of 2005, H.R. 4569, 109th Cong.; Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002).

Finally, we asked whether so-called "pirates" would be willing to pay *anything* for music. Against conventional wisdom, our results demonstrate that a large majority of pirates would be willing to pay something, granted far below market rate, to purchase music instead of illegally copy it.

Part II of this paper describes the analog hole with particular emphasis on the problem of signal degradation. Part III discusses the economics of music sales, focusing on the questions we sought to answer with our study. Part IV details our empirical research and results.

II. DRM AND THE ANALOG HOLE

A. Technical Overview

The analog hole is only meaningfully understood in the context of DRM. As the "D" in the acronym implies, DRM technologies operate exclusively on content in its digital form. DRM protects against unauthorized access, duplication, and distribution of digital content (e.g., audio and video), ensuring that such access to protected content is possible only under the conditions specified by the content owner.[2]

Although there are many disparate types of DRM, some generalizations will help motivate our discussion of the analog hole. Many DRM schemes rely on the introduction or injection by the content provider of extra data into the digital content stream or file, data that has nothing to do with the content itself.[3] For example, fingerprints[4] or watermarks[5] can be embedded into the digital copy of a song or movie, imperceptible to the end-user but detectable with DRM devices. These embedded codes can be used to authenticate a user's entitlement to play, reproduce, or distribute; to embed personal information to assist a future investigation; or to mark the data as free from tampering. After a DRM system identifies the fingerprint or watermark it can filter out or simply ignore the extraneous bits, thanks to the nature of digital data, leaving behind a perfect copy of the content. The listener or viewer will be unable in such a situation to detect any difference in the content.

2. *See* Eugene T. Lin et al., *Advances in Digital Video Content Protection,* 93 PROC. OF THE IEEE 171 (2005).

3. *See* Richard Owens & Rajen Akalu, *Legal Policy and Digital Rights Management*, 92 PROC. OF THE IEEE 997 (2004).

4. *See* Jürgen Herre, *Content Based Identification (Fingerprinting)*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 93 (Erberhard Becker, Willms Buhse, Dirk Günnewig, & Niels Rump eds., 2003); Daniel Schonberg & Darko Kirovski, *Fingerprinting and Forensic Analysis of Multimedia*, 2004 PROC. OF THE 12TH ACM INT'L CONF. ON MULTIMEDIA 788.

5. *See* L. Jean Camp, *DRM: Doesn't Really Mean Digital Copyright Management*, 2002 PROC. OF THE 9TH ACM CONF. ON COMPUTER & COMM. SECURITY 78.

The analog hole (also known as analog reconversion)[6] refers to an inherent vulnerability in DRM systems that makes otherwise protected material copyable by allowing it to be recorded as it is consumed.[7] The analog hole arises as an inevitable byproduct of the interface between computer technology and human biology. In order to sense (hear, see, feel) content in a digital form, it must first be converted into an analog signal. Visual images are converted from binary digits into signals that can be shown on a piece of display hardware (which typically uses light, via a LCD, LED, or CRT, to propagate the image through space to the human retina); sounds are converted from bits into signals that can be played, typically, using some kind of speaker (which converts the signal into compression waves in the air that travel to the human tympanum). If we lived in a world of science fiction, and we could "jack in" directly to our computers, comprehending the bits themselves, there would be no analog hole.

The inevitable conversion from digital to analog (typically performed using a specialized microchip called a digital-to-analog converter ("DAC"))[8] has two deleterious effects on DRM. First, the conversion process tends to strip away non-signal related information such as the fingerprints or watermarks relied upon by DRM. In fact, often the simple act of converting to analog and back again (using an analog-to-digital converter ("ADC"), naturally) will defeat DRM schemes.[9] Second, it is quite difficult to cram extraneous information inside the waveforms of an analog signal without affecting the perceived image or sound, so it is difficult to create DRM-like schemes on the analog side.

6. Many blanch at the term, "analog hole" for different reasons. Critics of legislation designed to "plug" the analog hole have said, "'Analog hole' is an artfully chosen term, referring to the fact that audio and video can be readily converted back and forth between digital and analog formats. This is just a fact about the universe, but calling it a 'hole' makes it sound like a problem that might possibly be solved." Posting of Ed Felten to Freedom to Tinker Blog, http://www.freedom-to-tinker.com/?p=954 (Jan. 12, 2006). Meanwhile, industry proponents of such legislation, perhaps hoping to move away from some of this stigma, describe it as "analog reconversion." *See* Susan P. Crawford, *The Biology of the Broadcast Flag*, 25 HASTINGS COMM. & ENT. L.J. 603, 619 (2003) (describing the Analog Reconversion Discussion Group ("ARDG")).

7. *See* Ross J. Anderson, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS (2001).

8. This DAC is the device that takes the quantized digital signal and returns it to an analog signal for transmission. To do this, the digital signal is decoded and stored in a buffer waiting to be sent to the speakers or headphone outputs.

9. Typically, the analog hole is exploited in two steps. First, an analog copy is created using a DAC; sometimes, but not always, this "intermediate copy" is saved, for example on videotape or cassette. Second, the analog copy is usually (but not always) converted back to digital using an ADC, which provides for the many advantages of digitally formatted information. For purposes of this discussion, both the intermediate copy and the final, digital copy will be referred to as "analog hole copies."

In other words, every conversion from digital to analog and every physical port, CRT, LCD, speaker, or wire through which an analog signal travels represents an opportunity to circumvent DRM. If a cable can be attached to a port, a video camera pointed at a CRT, or a microphone aimed at a speaker, a recording of the supposedly-protected content can be made. If the other end of the cable, video camera, or microphone happens to be attached to a computer, the unauthorized copy will be digital, suitable for high-quality and inexpensive mass duplication and redistribution over the Internet. Furthermore, unlike the arcane tools and skills required to circumvent DRM on the digital side, average consumers tend to be experienced with exploiting the analog hole, even if they don't know that's what they're doing. Consumers have been making copies from analog sources for years. The *Sony* case involved the use of videocassette recorders which were connected by consumers to analog television signals to record shows for future viewing.[10] Likewise, even average consumers (at least those born before 1990) can operate cassette recorders to copy music stored on CDs and vinyl records.

However, there is a significant limit to the uses of analog copying—signal degradation. First, each trip through an ADC or DAC degrades the signal, as information is lost in the process. For example, loss of stereo information and bass can occur, making a song sound like it is coming from inside a tin can. Distortion can also occur if the digital to analog converter supplies too much gain. Copies made using speakers and microphones may include ambient noise or distortion from the pass through the air gap.

The amount of degradation varies with the sophistication of the equipment used. For example, sophisticated reproduction equipment can be used to create relatively high-quality analog copies; large music companies use expensive and elaborate production facilities to mass-produce analog tapes. Such an operation requires a master recording specifically designed for longevity without significant degradation and special equipment to produce the tapes; however, this kind of high-quality mastering equipment and media is not generally available to the public at consumer pricing levels. This is one reason why large scale piracy by consumers in the pre-digital content age was never successful or lucrative.

In some sense, the analog hole can never truly be "plugged."[11] Those who talk about "plugging" refer to technical and legislative measures intended to make it more difficult to access and reproduce

10. *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 419 (1984).

11. *See* Felten, *supra* note 6. In other words, for video, even if every analog port on every device is sealed shut and every new video camera recognizes and refuses to record protected content, legacy video cameras will still be able to record the image.

analog signals. Developers are working on technical solutions that will embed watermarks in an analog signal that newer devices can recognize and refuse to record, including two complementary solutions known as Video Encoded Invisible Light ("VEIL") and Copy Generation Management System – Analog ("CGMS-A"). Older, less sophisticated systems such as Macrovision work a bit more crudely, essentially confusing the automatic gain control of VCRs, causing unwatchable reproductions. In addition, Congress has proposed legislation designed to mandate technologies like VEIL and CGMS-A to make the analog hole harder to exploit.[12]

There are many ways to exploit the analog hole to allow the recording of protected digital audio or video. Analog hole exploits can be separated into approaches "inside the box," which involve acquiring the signal from an internal wire, bus, or computer chip and often require advanced programming or electronics skills, and "outside the box" techniques which use external hardware, for example connecting two devices with a cable. Inside the box, signals can be captured directly from device buffers where the content is unprotected, or captured on its way to either an audio or video output device using capture hardware such as a video capture card. Although these techniques require a fair amount of skill, some software packages allow for easy inside-the-box copying. Outside the box, the content can be recorded using various analog capture devices including microphones and VCRs. The bottom line is that with the right equipment, one can sidestep DRM and reproduce the protected material with relative ease and little technical knowledge.

In fact, most standard computers, even relatively old ones, already possess all that is needed to generate a quick-and-dirty analog hole, digital copy: an audio card (with both "out" and "in" jacks) and audio file creation software packages, (available with standard operating systems). Simply run a cable from the speaker jack to the audio-in jack, push "play" on one music program and "record" on another, and you are exploiting the analog hole. There is an even more low-tech alternative—simply play the music through speakers and use a microphone attached to a recording device to copy the music as it plays. In either case, one then has the ability to produce an unlimited number of digital copies from the initial digital copy, thanks to a quick conversion to analog and back, albeit with some signal degradation.

12. *See* Digital Transition Content Security Act of 2005, H.R. 4569, 109th Cong. § 101 (proposed bill mandating use of VEIL and CGMS-A in all digital devices with analog outputs).

B. Legal Scholarship

Legal scholars have given scant attention to the analog hole. What is most often noted is the relationship between the analog hole, the DMCA, and fair use. In advocating for strict DRM anti-circumvention provisions in laws like the DMCA, content industry leaders have pointed to the analog hole as a good thing, as the safety valve protecting expression and fair use in a world without free digital copying.[13] Courts have embraced this reasoning, ruling that the analog hole provides breathing room to the DMCA necessary to preserve fair use and First Amendment rights.[14]

Several scholars have criticized this reasoning along two primary lines of attack. First, and more self-evidently valid, these claims are completely inconsistent with other claims made by the same content industries, sometimes contemporaneously, maligning the analog hole as a loophole around the DMCA that must be closed through regulation.[15] The other commonly voiced critique is that exploiting the analog hole is an imperfect safety valve for fair use and freedom of expression, because it is too costly,[16] too complicated,[17] or because of signal degradation.[18] Those raising these arguments provide no empirical support for the

13. *See* Gigi Sohn, *Don't Mess With Success: Government Technology Mandates and the Marketplace for Online Content*, 5 J. ON TELECOMM. & HIGH TECH. L. 73, 83 (2006) ("The presence of the analog hole is a common justification for greater limitations on fair use imposed by the anti-circumvention provisions of Digital Millennium Copyright Act."); Tal Z. Zarsky, *Assessing Alternative Compensation Models for Online Content Consumption*, 84 DENV. U. L. REV. 645, 661 (2006) (citing "DRM advocates" who "argue that existing loopholes in the DRM system [such as the analog hole] . . . would in fact allow users to exercise their right to fair use").

14. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 459 (2d Cir. 2001) (noting that the DMCA continues to allow one "to make a variety of traditional fair uses of DVD movies, such as . . . recording portions of the video images and sounds on film or tape by pointing a camera, a camcorder, or a microphone at a monitor as it displays a DVD movie"); 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085, 1102 (N.D. Cal. 2004) ("[U]sers can copy DVDs, including any of the material on them that is unavailable elsewhere, by non-digital means.").

15. *See* Crawford, *supra* note 6, at 618-21.

16. Zarsky, *supra* note 13, at 662 (suggesting that the analog hole is not a suitable substitute for fair use rights because "the tools for making digital copies of analog outputs are too costly").

17. *See* Alfred C. Yen, *What Federal Gun Control Can Teach Us About the DMCA's Anti-Trafficking Provisions*, 2003 WIS. L. REV. 649, 679 (noting that exploiting the video analog hole "requires the purchase of an appropriate camera and the effort of setting up the camera so that a serviceable image can be captured"); Zarsky, *supra* note 13, at 662 (suggesting that the tools that exploit the analog hole "require a high level of sophistication").

18. *See* R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619, 653 (2003) (arguing that analog hole techniques seem "likely as a practical matter to substantially diminish the quality and availability of such use"); Zarsky, *supra* note 13, at 662 (suggesting that exploiting the analog hole "might provide the relevant content in low quality").

claims of excessive cost, complexity and signal degradation. Instead, they tend to rely on intuition. By studying these three empirical questions—cost, complexity, and degradation—our study will give us the facts to bolster or refute these arguments.

III. ECONOMICS OF DIGITAL MUSIC AND THE COSTS OF DEGRADATION

Despite recurring claims by the content industry that analog hole exploitation will burden the market for their works, many questions must be analyzed before these claims can be assessed. Most importantly, given inevitable signal degradation, are analog hole copies truly market replacements for other, higher fidelity versions of the works? For music specifically, do analog hole copies of songs—made directly by users or downloaded from peer-to-peer networks—substitute for good-enough digital originals, such as compact discs or downloaded tracks? There are two extreme possibilities, with the likely truth somewhere in between. First, analog hole copy degradation may be so detrimental to listener enjoyment that no listener would consider an analog hole copy to be an acceptable replacement. If this is true, then the vulnerability will have no impact on the potential market for the digital originals. At the other extreme, the degradation problem may be wildly exaggerated, and analog hole copies may be good enough as not to hurt listener appreciation at all, meaning consumers will accept an analog hole copy as a perfect substitute for the digital original.

Assuming we establish that the consumer reaction to an analog hole-degraded copy falls between these two extremes, the next step is to ascertain the cost-quality relationship of these copies. If consumers are willing to tolerate analog hole-degraded copies if they are sold at a lower cost than a perfect digital copy, content owners may be able to take advantage of this tendency to price discriminate. Recent developments in the way digital music is sold provide a perfect platform to implement such a price discrimination scheme.

For digital music, an emerging business model is the pay-per-unit download, offered by services like Napster and iTunes. The music industry sells songs through these services for the price of 99¢ per download.[19] Chris Sprigman, in an article appearing earlier in this volume, provides a detailed, careful analysis of the 99¢ price point.[20] In particular, he wonders why virtually all songs are priced at this uniform price and specifically why the music industry has failed to price discriminate in setting prices for music downloads.[21] He suggests

19. *See* Chris Sprigman, *The 99¢ Question*, 5 J. ON TELECOMM. & HIGH TECH. L. 87, 88 (2006).

20. *Id.* at 90-94.

21. *Id.* at 89-90.

multiple song characteristics about which music companies could price discriminate: hit songs versus non-hits, old versus new, heavily restricted versus lightly restricted DRM.[22] Of most immediate interest is the idea of variable pricing based on audio quality.

Professor Sprigman speculates that music companies could increase sales and profits, and recapture surplus away from consumers by offering multiple versions of songs, at varying levels of quality, for varying prices.[23] "The audiophile who listens to music on his $10,000 home stereo may be willing to pay considerably more for a high-resolution digital file (which could easily offer better-than-CD-quality sound) compared with the casual listener who experiences music mostly through the cheap headphones of an iPod."[24] Despite this obvious market opportunity, he finds almost no indication of firms exploiting this form of price discrimination.[25]

Ultimately, he advances several theories for why downloads are not priced variably. Of particular interest, he considers, and apparently rejects, theories about consumer behavior.[26] These theories suggest that consumers would react unfavorably to the prospect of variable prices for different songs. For example, perhaps consumers would view the price differences to be unfair or confusing. In other words, these theories posit consumer resistance to variable pricing or, in reverse, a preference for the simplicity of the 99¢ price. It would be much easier to assess these theories if we knew more about consumer reactions to variable pricing based on quality differences.

Finally, our survey also explores the motivation of putative "pirates" of digital content. The conventional story is that pirates—those who obtain music online without paying anything for it—have become conditioned by the availability of free music against ever being willing to pay for music. In a related manner, Professor Sprigman attempts to tie the reluctance to move to variable pricing to a fear in the music industry of piracy and, in particular, peer-to-peer ("p2p") networks.[27] He speculates that if the record companies "attempt to charge too high a

22. *Id.* at 91-92.

23. *Id.* at 103.

24. *Id.* at 104.

25. Sprigman, *supra* note 19, at 104 ("While product differentiation by varying the bitrate of audio files might be a promising price discrimination strategy, we see little evidence of it.").

26. After rejecting consumer behavioral explanations, he seems instead to favor theories that involve the complex interplay between the oligarchical "Big 4" record companies, who control over 85% of music sales in the U.S., *see id.* at 95 n.12 and accompanying text, and Apple, Inc., whose iTunes Music Store dominates the industry, with approximately 83% of the U.S. market, *id.* at 95.

27. *Id.* at 115-16 ("[R]aising prices for hits above the 99¢ threshold may drive some who would otherwise be paying customers to unauthorized peer-to-peer downloading.").

price for premium content, they risk re-invigorating the p2p threat."[28] Again, this conclusion invites empirical analysis, because the interplay between the motives of those who use p2p networks to pirate copies is not well understood in the literature.

Many of these economic theories and assumptions are tested in the empirical study we describe below.[29] Measuring consumer response to quality degradation can support or refute Professor Sprigman's theories about possible price discrimination strategies for content owners. Studying the willingness to pay of putative pirates can confirm or rebut the widely-held conventional wisdom about the motives behind piracy.

IV. THE PRICE OF DIGITAL MUSIC

Can consumers perceive a difference between an original and an analog hole copy? How much is higher quality worth? At what price discount, if any, will a consumer accept lower quality? Are individuals who actively partake in digital music piracy willing to pay anything for music? Our study glimpses into the mind of the music consumer, attempting to quantify internal utility calculations in the cost/quality tradeoff. We note from the outset that our two surveys included only 70 and 90 participants, respectively, and that larger surveys should be completed to verify or refute our findings.

A. Simple DRM Circumvention with the Analog Hole

Our first goal was to assess, qualitatively and anecdotally, how difficult it is to create analog hole copies to circumvent DRM. If the analog hole is something that can be exploited only by the technically savvy user, it should perhaps be of little concern to the music industry. On the other hand, if the analog hole is easy to exploit, it supports industry claims (and refutes the contrary claims of some scholars) that it provides a meaningful safety valve for fair use and free expression in light of the DMCA. For music, we came to the latter conclusion. At least with current technology, the analog hole is very easy to exploit.

Our experiment utilized readily available software and hardware to make a copy of a digitally protected file. We created copies using two test-bed configurations, which we call the analog hole copy ("AHC") and the professional consumer copy ("PCC"). Both are outside-the-box approaches. The AHC was created by connecting the headset jack on a laptop to the audio-in jack on a desktop PC. The PCC was created by playing music out of a high-quality speaker (a home studio monitor) and

28. *Id.* at 117.

29. Although this research was completed before we knew of Professor Sprigman's work, it is a happy coincidence that these two efforts were contemporaneous with one another.

recording through a microphone across an "air gap."

For the AHC approach, setup took less than 15 minutes. Specifically, it took a few seconds to connect the laptop to the PC via a cable, less than five minutes to download and install software (called GoldWave) onto the PC, and another five minutes to install the same software onto the laptop. The most time-consuming element of this method was recording itself because the clips were simultaneously played and recorded in real time (e.g., it took thirty seconds to record a thirty-second clip). Finally, a software-based noise-reduction algorithm was applied at various levels to the captured clips using GoldWave; this final step again took only a few seconds. In total, it took about 45 to 50 seconds to record, noise reduce, and store a 30 second analog hole copy of the original music clip.

The PCC copying experiments used an Apple Mac G4 laptop with an M-Audio Mobile-Pre USB interface.[30] We played the clips out of Behreninger Truth near-field monitors and used two small diaphragm, Audio-Technica condenser microphones to record the music onto the same computer. The software used was Apple's "Logic Pro 6." This process also required only a few minutes to setup and a few minutes to create the copy.

The experiment showed that exploiting the analog hole for digitally protected music using readily available hardware and software is relatively easy, but mildly time-consuming. An individual intent on copying a large number of songs would be constrained by the amount of time it would take to record each piece of music. However, the GoldWave software has features that can speed up the recording time considerably, including double-time playback and double-time recording. We tested these settings and perceived no obvious quality difference. GoldWave also provides a batch feature which could be used to cue up a large number of songs for playback and recording. The batch copy is fairly sophisticated and could be used not only to copy, but also to apply the post-processing filters and even to place the final clip in the proper directory on the computer.

B. The Stated Preferences Surveys

We used the outputs—the analog hole copies—from our qualitative study as specimens for our surveys. The first survey was an econometric survey designed to assess what an analog hole-degraded copy of a protected digital file is worth. Thirty-second sound clips were used for the econometric survey. These were produced using the AHC and PCC

30. Professor Michael Theodore from the University of Colorado Department of Music created the PCC copies using his own equipment.

methods described above, introducing whatever degradation occurred in the ordinary course of the analog re-conversion. In other words, we took no additional steps to increase or decrease the "ordinary" level of degradation. Each respondent listened to a subset of the sound clips based on their listening preference from four music genres: alternative, country, oldies, and rock.

Through the survey, we sought to answer two questions: (1) is there a noticeable difference between the original and the copies? and (2) what is the economic value of the copies? For the first question, there was a fairly simple way to find the answer: play two snippets of the same song—one the digital original and one the post-analog re-conversion copy—for the respondent and ask which sample they preferred. The second question was more difficult to answer as it was not econometrically accurate simply to ask the respondent to provide a numerical answer. Instead, we had to extract this data in other ways.

In creating a survey, it is very easy to determine answers to questions such as, "Which do you prefer?" and "Have you ever done this?" Alternatively, the answers to "What is the value of this over that?" and "How do these aspects interact?" are far more difficult to ascertain. To answer these questions, an econometric model known as *stated preferences* was employed.[31] The main idea behind stated preferences is to ask consumers to indicate their preferences in a utility maximizing setting, or more simply, to have them indicate their preference for one option over another. By asking respondents to indicate their preferences in a series of questions, it is possible statistically to extrapolate important inferences relating the variables.

When applying this econometric method, it is important that every comparison between variables is made. This ensures that the relationships between variables are fully explored. This survey attempted to find the relationship between two variables—cost and quality—by asking people to indicate which audio clip they would rather purchase. Cost is a continuous variable (that is, there can be any value associated with it); however, using this method produces a discrete cost by limiting the number of options to two.

For example, after listening to two sound clips, labeled "Clip A" and "Clip B," the survey respondent was asked: "If Clip A cost $0.55 and Clip B cost $0.25 which do you prefer?" The survey varied both the prices and the clips, and each respondent was asked to assess every possible quality comparison available.[32]

31. *See* IAN J. BATEMAN ET AL., ECONOMIC VALUATION WITH STATED PREFERENCE TECHNIQUES: A MANUAL (2002).

32. In other words, with files containing music at three levels of sound quality–original, PCC, and AHC—there were nine possible comparisons made, including "comparisons"

Our statistical model relied on a few key themes. People make decisions to maximize their utility (personal value). Relying on this basic economic rule, statistics can be used to create various models to assign a probability to a respondent's choice. These probabilities allow determination of the respondent's evaluation of the importance of the two variables.

The survey itself was conducted using Zoomerang,[33] an Internet survey application.[34] The survey collected responses from 70 participants. Of those, 66 completed the music portion of the survey. Demographically, the respondents were either current and former graduates of the University of Colorado's Interdisciplinary Telecommunications Program or engineers and computer scientists working for a local technology firm. The respondents varied in age from 18 to 63 years; the median age was 28 and the mean age was 30.

C. Results and Analysis of the Surveys

Our analysis centered on the following two questions: (1) do consumers perceive a difference between analog hole copies and originals? and (2) at what cost will the consumer be willing to sacrifice some quality?

With respect to the first question, based on the number of times the digital original was picked as preferable to the analog hole copy, it appears that respondents preferred the original clips to the analog hole copies, but not by as wide a margin as we had originally expected. Specifically, when respondents were asked whether the clips were of the same quality or if one was of superior quality, the original was picked approximately 52% more often than the AHC and 42% more often than the PCC copies.

To answer the second question, an econometric survey using the approach described above was conducted. As discussed earlier, the model was designed to ask consumers to indicate their preferences in a utility maximizing setting. In this case, a random utility model was applied. The trade-off between cost and quality was the change in utility with respect to quality divided by the change in utility with respect to price.[35]

---

between identical versions. During the survey, each respondent received each one of the nine possible permutations to compare, with randomly assigned prices for each song in the pair.

33. Zoomerang, http://info.zoomerang.com (last visited Mar. 22, 2007).

34. Zoomerang was created in 1999 by MarketTools to provide online survey services that are accurate and comprehensive for minimal cost and effort. Zoomerang, About Us, http://info.zoomerang.com/company.htm (last visited Mar. 22, 2007). This program allows flexibility and originality in survey creation. One is able to choose the type of question as well as provide answer choices and randomization.

35. While the details of this econometric study are beyond the scope of the paper,

The results of the study indicate that the survey respondents place a value of 24¢ on the difference in quality between an original and an analog hole copy. In other words, for this group of respondents, there was a perceived quality difference between the original and the copies, and the respondents were willing to pay 99¢ for the original and 75¢ for the copy.

These results support the claim that the music industry should attempt to capture new market segments by releasing different quality versions of their digital content.[36] Specifically, if these results are generalizable, the market for digital copies of music could be segmented with a standard quality song retailing for 75¢ per download.[37] This price point could encourage consumers who are unwilling to pay the current 99¢ price for "superior quality" copies to purchase cheaper, "standard quality" downloads instead.

D. Will Pirates Pay for Digital Music?

In a follow-up survey, we studied the willingness to pay of so-called "pirates," which we defined as people who obtained most of their music through illegal file-sharing.[38] The goal was to determine if there was a price point at which even a pirate would abandon piracy and begin to pay for music. We surveyed 90 users of pirated music. To focus on those least likely to pay anything for music, we also required that they had not paid for any online music in the last six months. Demographically, every respondent turned out to be undergraduate or graduate student at the University of Colorado between the ages of 18 and 25.

Among this sample population, we found a bimodal distribution. Twenty percent of these individuals were not willing to pay anything for the music. However, the remaining 80% were willing to pay from 20 to 40¢ for a legal download, instead of obtaining copies from non-paid sources.[39] This is a very interesting finding and suggests that alternative

interested readers should contact douglas.sicker@colorado.edu for the details.

36. *See supra* Part III. Professor Sprigman's suggestions, discussed *supra*, about varying price with quality focused in particular in varying the bitrate (roughly speaking, the higher the sampling bitrate, the higher the quality of the track) and file format (e.g., mp3, aac, and ogg). *See* Sprigman, *supra* note 19, at 103-04.

37. iTunes already produces a lesser-quality content download.

38. The exact question we used to screen respondents was: "Would you say that most of your digital music collection was obtained through illegal file sharing? If so, please answer the following questions."

39. Interestingly, this may be an economically feasible price range. eMusic, an online service that sells downloads from independent record labels, charges $10 for 40 songs, or 25¢ per song. *See* Sprigman, *supra* note 19, at 111. Professor Sprigman finds the difference between this price and the major labels' 99¢ price to be some evidence of the exercise of market power by the majors. *Id.* If he is correct, perhaps 20¢ to 40¢ is within the range of the competitive, market-clearing price that would exist absent this market power.

pricing models might be able to capture these individuals. We also gave the respondents space to comment on why they would prefer to purchase instead of pirate. Aggregating these answers, they appear generally motivated by three things: the desire to own content legally, the convenience of being able to more easily find desired content, and the guarantee of a high-quality product. We also asked the survey respondents for their thoughts about DRM. Eighty percent indicated that were they to purchase music, they would want the flexibility to move the music onto different media players or to control and access it in various other ways.

V. CONCLUSION

Our results suggest some untested pricing methods for minimizing the impact of digital piracy. We have shown that consumers are willing to price differentiate on quality and that would-be pirates are willing to pay for content, albeit at a significantly reduced price. These results all point to lost opportunities for the music industry. Price discrimination based on quality can increase sales, profits and seller surplus. The community of pirates may be "brought back into the fold" if the 80% who are willing to pay can find a market.

We have also filled in empirical gaps in the debate over the analog hole. The analog hole can be easy to circumvent, at least for music. Furthermore, although analog hole exploits tend to lead to detectably degraded copies, many ordinary consumers will not notice the difference. This also supports industry fears that analog hole copies may serve as a market substitute for DRM-protected digital copies.

The survey sample sizes we used were not large enough to reach external validity for applying these results to the general population. Looking forward, a next step would be to execute a similar survey to the one administered for this paper but on a much larger scale. Also, tailoring surveys specific to demographics such as socio-economic, age, ethnicity, and gender could yield insightful and perhaps unexpected results.[40] Although we focused on music, similar research in copying and distributing video should be examined as well.

40. It is likely that our sample of college-aged students at the University of Colorado represents a very stratified sample.

THE NEED FOR SOFTWARE INNOVATION POLICY

CHRISTOPHER RILEY*

This paper examines the current legal treatment of software innovation. It argues that recent judicial standards for the regulation of software innovation do not adequately protect innovation. It presents an original standard for the regulation of software innovation, one intended to guide judicial decisions in contributory copyright liability, in interpretations of the Digital Millennium Copyright Act, and in every courtroom where a developer is on trial for the mere creation and distribution of software. The standard presented in this paper separates the questions of liability and remedy in order to produce an optimal dynamic balance of interests.

* Ph.D., Computer Science, Johns Hopkins University, 2004; J.D. expected, Yale Law School, 2007. I would like to thank Professor Jack Balkin, James Grimmelmann, Eddan Katz, and the attendees of the Yale/Harvard Cyberscholar Working Group for their helpful comments.

I. INTRODUCTION

Peer-to-peer filesharing networks like Napster and Grokster are considered a blight on society by the media and copyright holders. They have enabled millions of people to acquire music for free, without paying any royalties or license fees. The users of these programs have broken the law; few would dispute that.[1] The Supreme Court and other courts have held that the producers of the network software also violated the law, under the doctrine of secondary liability for copyright infringement.[2] As a result, these software innovations have been restrained – the developers have stopped distributing their systems, or have converted them into industry-sanctioned subscription services.[3] And the industry continues to fight, to challenge the distribution and use of new generations of filesharing systems.[4]

Let us suppose for a minute that all of this could have been avoided, that before the very first peer-to-peer filesharing network had been released to the public, the copyright industry could have taken its developer into court. Determining that these programs could be used to exchange music files in violation of copyright law, and that this possibility was known to (perhaps even intended by) the developers, the court would have enjoined the distribution of the software, threatening the developers with damages should the systems be used to exchange copyrighted files without permission. The public would never have seen the network, and would not have realized that such forms of communication were possible. Without seeing first-hand the efficiency, portability, and audio quality of MP3-encoded music files, society might not have developed the necessary demand to make the (very expensive) portable MP3 player a market success. We would not have online music stores, such as iTunes, which were developed as legal alternatives to

---

1. At least one person has tried this argument in a court of law. BMG Music v. Gonzalez, 430 F.3d 888, 891 (7th Cir. 2005), *cert denied*, 126 S. Ct. 2032 (2006) (upholding a district court verdict that as a matter of law filesharing did not constitute fair use).

2. Secondary liability is a common law doctrine that penalizes the distributor of a device used by others to infringe copyright. It is often used when punishment of the direct infringers is not feasible. *See, e.g.*, MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 929-30 (2005).

3. The original filesharing service, Napster, has converted into a monthly subscription service, in which users can pay a flat monthly fee and stream music from Napster's catalog. Napster, http://www.napster.com/ (last visited Feb. 13, 2007).

4. One of the major companies offering BitTorrent files, LokiTorrent, attempted to collect donations to fund a legal team to fight the Motion Picture Association of America. *See* Robert Lemos, *LokiTorrent Fights MPAA Legal Attack*, CNET NEWS.COM, Dec. 30, 2004, http://news.com.com/2100-1025_3-5508073.html. They raised $40,000, but the site administrator still agreed to comply, paying a small legal fine and shutting down the service. *See* Michael Ingram, *LokiTorrent Caves to MPAA*, SLYCK NEWS, Feb. 10, 2005, http://www.slyck.com/news.php?story=661.

peer-to-peer networks. Eventually, of course, the major market players might have figured out the strong potential market of online music distribution. But the pace of innovation would have been greatly slowed without competition.

The potential harm to the computer science industry would have been even worse than the harm to the consumer market. Computer scientists and engineers took the ad-hoc, highly distributed model of peer-to-peer networking and adapted it in many ways, creating systems such as SETI@Home for distributed computation or IRIS for distributed storage.[5] Peer-to-peer systems have many technical advantages over traditional client-server systems, including: increased scalability (the capacity of the system to increase the number of participants with low overhead), fault tolerance (the ability of the system to continue functioning even if many individual participants fail), and flexibility (the ability of the system to adapt to serve multiple functions).[6] Again, perhaps these advantages would have been realized eventually. But peer-to-peer filesharing networks brought them to society more quickly, more widely, and at less cost.[7]

This is the story of one innovation, and of what would have been lost if the legal system had cut it off in its incipiency. Peer-to-peer networks and other technological innovations produce transformative effects on our society, both good and bad. Many everyday technologies were themselves once radical technological innovations, such as the

---

5. SETI@Home (SETI stands for "Search for ExtraTerrestrial Intelligence") uses volunteer contributions of idle computing cycles from home personal computers to analyze satellite data. *See* SETI@home, http://setiathome.ssl.berkeley.edu/ (last visited Feb. 11, 2007). The Infrastructure for Resilient Internet Systems (IRIS) project is a collaborative effort of academic computer scientists from five universities to build distributed systems based on Distributed Hash Tables, or DHTs, a structure fundamentally based on the peer-to-peer communications model. *See* IRIS: Infrastructure for Resilient Internet Systems, http://project-iris.net/index.html (last visited Feb. 11, 2007). Many IRIS papers were published at the annual International Workshop on Peer-to-Peer Systems (IPTPS). The first academic Distributed Hash Table, the Chord system of Stoica et al., was published in 2001. Ion Stoica et al., *Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications*, PROC. OF THE 2001 CONF. ON APPLICATIONS, TECHS., ARCHITECTURES, & PROTOCOLS FOR COMPUTER COMM. 149, *available at* http://pdos.csail.mit.edu/papers/chord:sigcomm01/chord_sigcomm.pdf. Contrast this with the Napster peer-to-peer filesharing network, which by 2000 had already reached a federal court. *See* A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part*, *rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

6. *See, e.g.*, Rodrigo Rodrigues, Barbara Liskov & Liuba Shrira, *The Design of a Robust Peer-to-Peer System*, 2002 PROC. OF THE 10TH ACM SIGOPS EUR. WORKSHOP: BEYOND THE PC 117, *available at* http://pdos.csail.mit.edu/papers/chord:sigcomm01/chord_sigcomm.pdf.

7. The distributed development of peer-to-peer networks by amateurs is of lower cost to society than academic research, which is funded largely through taxpayer money in the form of grants. Many scholars have praised the collaborative development environments through which these programs are created. *See, e.g.*, YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

home VCR, with both good and bad effects. These fundamental innovations might have been permanently barred from the world if past courts had not been so open-minded.[8] Similarly, the amateur programmers and would-be inventors, like the graduate students who founded Google,[9] might never have built their world-changing systems if they feared multimillion dollar legal judgments against them based on unanticipated and undesired secondary uses of their products. No one can imagine what the world would look like today had these innovations and others been prohibited. Nor can anyone accurately imagine future technologies or how the courts will react to them, to know what lies on the horizon of the regulation of innovation. But hopefully I have created a suspicion that the risks of overly restricting technological innovation are great.

In the modern era, software innovations – innovations that take the form of new, original computer software programs, or new uses or combinations of existing computer programs – exaggerate the transformative effects of general technological innovations because of their potential for rapid, low-cost development and fast, widespread deployment. Innovation in the computing industry is not a story of patent law and the research and development divisions of multimillion dollar corporations. The real history of Silicon Valley is not a story of the modern-day IBMs and Microsofts, armed with advertising executives and teams of lawyers, but of garage inventors and students with great ideas who were given the freedom to pursue them without fear of legal reprisal.[10] These entrepreneurs operated under only the constraints of technology and the bounds of human imagination.[11] Their innovations broke new ground in the technology industry. Low barriers to entry and a tradition of commercial success engendered a world of small "startup" companies and of individual hobbyists and tinkers. These small

8. The U.S. Supreme Court was faced with this issue in the landmark 1984 case concerning the legal status of the Sony Betamax video recorder, and it chose to interpret existing secondary liability laws in copyright to protect the innovation against established legal interests. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

9. Google Corporate Information: Management, Larry Page, http://www.google.com/corporate/execs.html#larry (last visited Mar. 26, 2007); Google Corporate Information: Management, Sergei Brin, http://www.google.com/corporate/execs.html#sergey (last visited Mar. 26, 2007).

10. Hewlett-Packard is one of the original garage companies, started by Dave Packard and Bill Hewlett in the late 1930s. *See* HP Company Information, HP History: HP Timeline – 1930s, http://www.hp.com/hpinfo/abouthp/histnfacts/timeline/hist_30s.html (last visited Feb. 12, 2007). More recently, search engines Yahoo and Google were both created by graduate students as little more than hobbies. *See* Rank for Sales, How Yahoo Was Founded, http://www.rankforsales.com/n-ay/719-seo-aug-18-04.html (last visited Mar. 26, 2007); Wikipedia, Google, http://en.wikipedia.org/wiki/Google (last visited Feb. 12, 2007).

11. Professor Lessig has analyzed the distinctive role of technological constraints on innovation. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

innovations, many of which may have seemed unimportant at their conception, have led to amazing social benefits. Yet these innovations in particular are threatened by the current, heavily risk-averse and pro-corporation legal climate for technology law.

Many software innovations create enormous benefits and enormous harms. They interfere with existing corporate and government interests, and are challenged through the legal system as a result. Legislatures create new laws and courts extend existing laws to contain this interference. Some of the legislative actions, such as restrictions on the sending of unsolicited commercial e-mail,[12] correct clear, widespread social problems. Others, such as the Digital Millennium Copyright Act of 1998, serve narrower corporate interests, and place undesirable restrictions on legitimate activity.[13] Rarely does freedom win in the battle against legal incumbency.[14] The courts have followed a similar pattern. In *Grokster*, the most recent major judicial statement on the regulation of innovation, the Supreme Court introduced a new theory of copyright liability, inducement, to restrict the activity of software developers.[15] The courts occasionally but rarely introduce exceptions.[16] As a result of this tightening, innovators face strict, yet vague controls over the functionality of their developments, and they fear that they may face injunctions or even massive statutory damages.

The balances of interests drawn by cases such as *Grokster* are far from optimal, because they are *static* balances. Courts consider only the current benefits and harms of software, and do not take into account long term and external costs of regulation to the innovator and to other innovators. These errors of judgment result in a balance that, generally, overvalues damage to legal interests and undervalues damage to innovation.[17] Fixing the squeaky wheel in this case greatly reduces

12. Federal and state laws restrict the sending of spam. The federal law is the CAN-SPAM Act. *See* CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701-7713). California, among many other states, also has a thorough anti-spam law. CAL. BUS. & PROF. CODE § 17529 (West 2004), *available at* http://www.spamlaws.com/state/ca.shtml.

13. *See generally*, Jeffrey D. Sullivan & Thomas M. Morrow, *Practicing Reverse Engineering in an Era of Growing Constraints Under the Digital Millennium Copyright Act and Other Provisions*, 14 ALB. L.J. SCI. & TECH. 1 (2003).

14. One well-publicized example is the Family Movie Act of 2005, part of the Family Entertainment and Copyright Act of 2005, which amended federal copyright law to allow technological blocking of non-family-friendly portions of movies. *See* Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, 119 Stat. 218 (codified as amended in scattered sections of 2, 17, 18, 28, and 36 U.S.C.).

15. *Grokster*, 545 U.S. at 936-37.

16. The most significant of these is the *Sony* safe harbor, an exemption from contributory copyright liability for the distributors of devices that possess "significant non-infringing use." *Sony*, 464 U.S. at 442.

17. One might argue that this approach is justified because the future benefits of

future social value.

Regulation must be made under the guidance of a broad innovation policy, one that considers not only the observable infringing and non-infringing uses of software, but also the effects of constraints on future innovation. The concerns of software innovation policy overlap with those of intellectual property, the First Amendment, contract law, and antitrust. But it is distinct from these, as it serves different goals and is concerned with different risks, and it deserves independent consideration. Software innovation policy must protect the benefits of new software innovations while limiting the harms of those innovations, and it must preserve an open and unconstrained environment for innovation, free from undue chilling effects and other powerful disincentives.

I propose that the legal system resolve these conflicting interests through a two-part standard. First, the benefits and harms of the innovation itself, and the benefits and harms in the repercussions of the decision to prohibit or to permit the technology, are balanced, in order to decide whether society is better off, now and in the long term, with or without the innovation. This is the *liability rule*, intended to determine, as an initial matter, whether or not the innovation should be permitted or controlled. The liability rule is dynamic – it looks not just at the current uses of the innovation (the static considerations emphasized by current law), but also at foreseeable future uses, and at the external costs and benefits of regulating or permitting the innovation. Second, and only if the answer to the liability rule is to prohibit the innovation, the intent of the developer is examined to determine whether the appropriate remedy is to enjoin continued development and distribution of the innovation, or to hold the developer responsible for damages. This is the *remedy rule*, designed to structure the legal response to liability in a manner that is neither under- nor over-broad. By separating the legal standard into liability and remedy, and by using proper rules at both levels, the courts can make a clear and correct decision at to whether the technology should be permitted (without using the developer's motive as a proxy for proper decision, as the Court in *Grokster* does), and can structure the remedy in a manner that does not create excessive chilling effects by making other well-intentioned developers fear massive damages.

In this paper, I develop these issues further. In section II, I explain why software innovation is at risk and why it must be protected. In

innovation are speculative and therefore not appropriate for judicial decision-making. There are two compelling reasons not to follow this theory here. First, simply ignoring the prospect of future innovation is absurd, and the consequences would be severe. Second, some types of non-specific long-term harm to innovation, such as the imposition of chilling effects on future developers, can be avoided easily through proper policy, such as the proposal presented in this paper.

section III, I give more detail on the current legal system's approach as established by *Grokster*. I argue that *Grokster* is both over- and under-protective, and I propose a two-part liability-remedy standard that accurately protects innovation. In section IV, I discuss and criticize a number of alternative proposals for the protection of innovation, including expansive readings of copyright's fair use exception and of the First Amendment, and I address potential challenges to my standard.

II. WHY MUST WE PROTECT SOFTWARE INNOVATION AND HOW IS IT AT RISK?

A. Why is Software Innovation Different from Other Forms of Innovation?

Software innovation stands apart from other forms of innovation in many ways. The first of these is discussed in almost every work dealing with the new digital era: the marginal cost of additional copies of the technology is negligible. This is, of course, one of the primary reasons for the creation of intellectual property rights in the first place – the creator cannot internalize the benefits of the technology if the creation of additional copies cannot be controlled and formed into a market, and thus the creator has a greatly reduced incentive to innovate.[18] Redistributing software products is fundamentally different from redistributing physical property, such as a piece of furniture, or many other goods protected by intellectual property, such as textbooks. While a textbook can be reproduced by a photocopier, the labor requirements of this process make mass redistribution impractical, unlike the negligible cost of uploading and downloading a digital file.

There are other major differences as well. As mentioned earlier, the scale of effort and time required to create most software programs is nowhere near the scale required to create other types of innovations. Consider pharmaceuticals – laboratories spend years and millions of dollars on development and testing, and still many of their creations end up being unusable or unmarketable. The industry relies on the blockbuster drug in order to survive. Software development, in contrast, happens in large part by individuals, even hobbyists.[19] Sure, there are some notable larger products, such as Microsoft's Windows operating system. But even large software programs such as operating systems can

18. *E.g.*, WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 11 (2003) ("Because intellectual property is often copiable by competitors who have not borne any of the cost of creating the property, there is fear that without legal protection against copying the incentive to create intellectual property will be undermined.").

19. *See, e.g.*, How Yahoo Was Founded, *supra* note 10.

be (and are) created by amateurs, because the development process can be distributed across widely dispersed individuals.[20] Furthermore, software innovation is often a highly collective phenomenon, in which the freely exchanged code and ideas help others with their innovations.[21] These structural features of the process of innovation in software render it prone to crippling regulation – for many innovations there are no companies with teams of lawyers and large capital investments worth defending. Instead, software innovators are often amateurs with many other things going on in their lives, who lack the necessary cohesion and economic motivation to lobby legislators and administrators to shape the law in their favor.

Perhaps the biggest and the most salient difference between computer software and other forms of innovation lies in its adaptability to both socially beneficial and socially harmful uses. Software programs may be created for a single purpose, or for no purpose at all, merely to express some creative impulse of the programmer. But others can later adapt these same programs, either through additional programming or simply through unintended usage, to perform functions beyond those imagined by their programmers. In other words, the original intention of the programmer and the original uses of the program are not enough to form a complete evaluation of the program's overall social utility, complicating further the ability of a primarily backward-looking legal system to resolve equity questions concerning software programs.

Finally, the law treats software innovations differently than other forms of innovation. With most technological innovations, patent law serves as the primary legal control. In software development, on the other hand, copyright law, patent law, and focused statutes such as the Digital Millennium Copyright Act all play major governing roles. Copyright law's fair use provisions and the First Amendment have also had significant impact on software development and use. Even beyond these formal legal systems, software programs come equipped with End-User License Agreements, which use contract law to place additional restrictions on the use of a product. This quagmire of assorted laws places a variety of substantively different limitations on the development

20. The Linux operating system is the classic example of this. *See, e.g.*, Yochai Benkler, *Coase's Penguin, or Linux and the Nature of the Firm*, 112 YALE L.J. 369, 406 (2002).

21. Isaac Newton famously wrote, "If I have seen further, it is by standing on the shoulders of giants." Letter from Sir Isaac Newtwon, Trinity College, to Dr. Robert Hooke (Feb. 5, 1675) *in* SIR DAVID BREWSTER, MEMOIRS OF THE LIFE, WRITINGS, AND DISCOVERIES OF SIR ISAAC NEWTON 142 (1855). Many modern scholars have written on the role of the commons in modern information production. *See generally* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001); Benkler, *supra* note 20, *passim*.

of software, and leaves little room for the protection of software in and of itself, as a matter of policy. A separate, independent examination of the nature of software innovation, and of what must be done to protect it, must be conducted outside the doctrinal boundaries of any individual source of regulation.

B. Why is Software Innovation Valuable?

The value of the computing industry as a whole should not need to be argued. The value of innovation, on the other hand, deserves some elaboration. Continuing software innovation confers a number of benefits on the computing industry. Some innovations create new ways in which computing better organizes and makes available information from the outside world.[22] Some improve on existing functionality, either by reducing inefficiency[23] or by improving correctness.[24] Many add new features to existing essential products.[25] These benefits enable the management of ever more data from the outside world, leading to faster and more reliable communications, more powerful computations for scientific applications, and improved efficiency in all operations from hospitals to warehouses to personal computers. To continue creating new social benefits, the computing industry requires a sustained high level of innovation, to keep up with the increasing sources, uses, and amounts of data that must be processed.

Promoting small innovators, in particular, supports a number of other related social values. For example, many legal scholars are studying peer production, a less hierarchical, more fluid and collaborative form of production of knowledge goods.[26] Peer production

---

22. Google Book Search, for example, adds new functionality to the industry. Google Book Search, http://books.google.com/ (last visited Mar. 26, 2007). While the concept of scanning a book is not new, I contend that creating a searchable database of the text of many books is a new and valuable innovation. *See infra* Part II.E.4.

23. Consider the development of the MP3 audio encoding, which permits far more compact storage of high quality audio music. *See, e.g.*, Mp3licensing.com, About mp3, http://mp3licensing.com/mp3/index.html (last visited Mar. 26, 2007).

24. Ongoing improvements in speech recognition software, for example, provide continually more accurate transcriptions. *See, e.g.*, Posting of Amit Agarwal to Digital Inspiration Blog, http://labnol.blogspot.com/2007/01/dragon-naturallyspeaking-9-speech.html (Jan. 22, 2007).

25. Consider journaling file systems such as Redhat's ext3, which serve the same purpose as ordinary file systems, yet implement this purpose in a way which adds new logging to increase reliability. Michael K. Johnson, Whitepaper: Redhat's New Journaling Filesystem: Ext3, http://www.redhat.com/support/wpapers/redhat/ext3/ (last visited Mar. 26, 2007); *see generally* Wikipedia, Journaling File System, http://en.wikipedia.org/wiki/Journaling_file_system (last visited Mar. 26, 2007).

26. *See, e.g.*, Benkler, *supra* note 20, at 375-378 (describing in detail the ability of peer production to organize and produce effectively despite its decentralization and lack of formal incentives relative to the traditional Coasean model of the firm).

improves the quality and speed of software development, increases the diversity of viewpoints in the media landscape, and promotes a cultural democracy.[27] Many digital innovations are peer produced, most notably the Linux operating system.[28] If the legal system does not protect innovation, peer production will lose the tools and the freedom it requires, and many valuable innovations will be lost.

Amateur participation in software development also helps to correct the digital divide.[29] Hobbyists, from the United States and from abroad, need only a computer and an Internet connection in order to produce and distribute their own software. A software business can be started without taking out loans to acquire capital, establishing real estate, and hiring employees. Software innovation also helps and is helped by the Access to Knowledge movement.[30] The A2K movement, in part, works to ensure that the information and tools needed to innovate are widely available;[31] but, also, the protection of software innovation preserves freedom to acquire and share knowledge (because amateurs feel free to develop and distribute their own software) and enables the development of communications and management tools necessary to share and organize information, advancing the A2K movement in return.

C. What Will We Lose if We Do Not Protect Software Innovation Adequately?

Prohibiting innovation steals from society any beneficial value of that innovation. Many challenged (or challenge-able) software innovations provide considerable social benefits. For example, the Tor network provides anonymity, which can be used to disguise the identities of copyright infringers, but can also be used to preserve privacy and the freedom of speech.[32] As another example, the creators of the BnetD server may have violated the terms of a license agreement, but they created a program that encourages competition by offering a valuable

---

27. For more on democratic culture and the Internet, s*ee, e.g.*, Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1 (2004).

28. While in this sense innovation benefits from peer production, peer production also depends on good innovation policy. Full exploration of the synergy between these movements is beyond the scope of this paper.

29. The "digital divide" is the social rift between those who can use and benefit from high technology and those who cannot. *E.g.*, Digital Divide.org, Digital Divide: What It Is and Why It Matters, http://www.digitaldivide.org/dd/digitaldivide.html (last visited Apr. 4, 2007).

30. *See, e.g.*, Posting of Jack Balkin to Balkinization, http://balkin.blogspot.com/2006/04/what-is-access-to-knowledge.html (Apr. 21, 2006).

31. *Id.* (noting that components 2 and 4 of the typology of "access to knowledge" are "Information" and "Tools for the production of knowledge-embedded goods").

32. The Tor system is discussed in more detail in Part II.E. *See infra* notes 76-77.

alternative to Blizzard's official video game servers.[33] If these technologies are too constrained, society will lose their benefits as a consequence of avoiding their harms.

Some technologies that support both benefits and harms should be prohibited, and some should be permitted. Society is not best served by turning a blind eye to the harms of technology, to preserve its benefits regardless of the consequences. The inability to predict the future combined with the harm of letting the technology go through a "trial period" makes infeasible any policy that never prohibits innovation.[34] But if the perceivable beneficial use of a technology is sufficient, then society will lose a great deal of value if the technology and the developer are not protected against legal challenges.

Beyond depriving society of the benefits of the individual innovation, broad regulation produces more peripheral (but no less severe) damage in the form of chilling effects. A chilling effect in the First Amendment context occurs whenever a vague regulation on activity, enforced by criminal sanction, provides too strong an incentive for a legitimate speaker to remain silent out of fear of prosecution.[35] In the context of technology law, one can imagine an analogous chilling effect, in which software developers fear production and distribution of their software because it may trigger liability under copyright law or the Digital Millennium Copyright Act.[36] This concern is made especially ominous by copyright law's severe financial penalties for infringement.[37] The fear of large damage awards empowers rights holders to threaten enforcement of existing laws beyond their actual scope through the use of "cease and desist" letters.[38] As applied to innovation, chilling effects

33. The BnetD system is discussed in more detail in Part II.E. *See infra* note 64.

34. Consider, for example, a software virus. In theory, it is possible that a software virus may lead to future social benefits, such as an increased investment in security or an increased awareness of computer security. But this is too long-term and too speculative, and certainly insufficient to justify permitting a virus to cause harm for a while, just to see if it eventually produces beneficial use.

35. *See, e.g.*, Reno v. ACLU, 521 U.S. 844 (1997).

36. To settle multiple lawsuits against them, Niklas Zennstrom and Janus Friis, the developers of the Kazaa file sharing system, agreed to pay $125 million in damages. Jeremy W. Peters, *Kazaa's Creators Do Latest Venture by the Book*, N.Y. TIMES, Feb. 27, 2007, *available at* http://www.nytimes.com/2007/02/27/technology/27joost.html.

37. *See, e.g.*, Fred von Lohmann, Electronic Frontier Found., Remedying Grokster, July 25, 2005, http://www.eff.org/deeplinks/archives/003833.php ("much of the copyright chill felt by innovators and technology investors can be traced to the prospect of apocalyptic statutory damages that can reach beyond the corporate grave into the personal assets of officers, directors and investors."). Statutory damages in copyright law range from $750 to $30,000 per infringement. 17 U.S.C. § 504(c)(1) (2000). The chilling effect is also amplified by the prevalence of amateur innovators, who would not have the resources to pay attorneys to defend a legal challenge, much less survive a losing decision.

38. The Chilling Effects Clearinghouse, http://www.chillingeffects.org (last visited Feb. 13, 2007) (project is collecting and publishing these letters to increase public notice of First

are generated whenever an innovator is held liable solely for the functional features of the innovation. The best example of this in case law is *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001). Nothing like the Napster service had existed before; while the developers might have suspected their service was illegal, there was no way for them to know. In the future, an innovator who fears retribution may refrain from creating and distributing software that is actually legal and valuable for society.[39] What society loses from overregulation, then, is the social value of these foregone innovations.

D. The Legal Climate for Innovation

While software patents exist, the greatest restrictions on software innovation come from copyright law and the Digital Millennium Copyright Act.[40] Since it was passed in 1998, the Digital Millennium Copyright Act has served as one of the most popular legal tools to stifle innovation and competition in the technology industry. The DMCA prohibits the circumvention of a technological protection measure used to protect copyright.[41] The DMCA creates a legal obstacle to technological arms races – sequences of maneuvers where security mechanisms broken by third parties are replaced by stronger mechanisms which are themselves broken. But many private parties have tried to use the law to stifle legitimate competition. It has been used (not always successfully) to challenge generic ink cartridges,[42] video game servers,[43] and garage door openers.[44] These attempts demonstrate the risks that the DMCA poses to innovation, risks that were only briefly acknowledged during the bill's passage.[45] And the legislators' minor nods towards the

---

Amendment and intellectual property rights).

39. Note that, in contrast to First Amendment chilling effects, this conception of chilling effects has considerable utilitarian value. While the direct effect is on the innovators who fear legal retribution, the ultimate loser is society, which is deprived of the benefits of the innovations that would otherwise have been created.

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

41. 17 U.S.C. § 1201(a) (2000).

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

43. *See, e.g.*, Davidson & Assoc., Inc. v. Internet Gateway (Internet Gateway II), 422 F.3d 630 (8th Cir. 2005).

44. *See, e.g.*, Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

45. In comments on what would become 17 U.S.C. § 1201(f), an exception for activities constituting reverse engineering for the purpose of creating interoperable products, Senator Orrin Hatch stated that "[t]he purpose of this section is to foster competition and innovation in the computer and software industry." S. REP. NO. 105-190, at 13 (1998). Then-Senator John Ashcroft appeared concerned that the statute might be interpreted to mandate technology design, "which would have a dampening effect on innovation." 144 CONG. REC. S4890 (daily

value of innovation have been overshadowed by the practical applications of the bill and by other legislative action, such as the oft-attempted Broadcast Flag bill.[46]

Copyright law prohibits direct infringement in software development (e.g. by copying and using source code from one program to another without permission). Common law (based on copyright law principles) also prohibits secondary infringement, such as the development of a software tool that is used by others to infringe copyright. Historically, secondary infringement doctrine had two separate grounds for liability, contributory and vicarious. Contributory liability requires that a software developer "knowingly" and "materially" provide assistance to a direct infringer.[47] Vicarious liability requires a developer to have a "financial interest" in the infringement and have "the right and ability to supervise" the infringing activity.[48] In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), the Supreme Court added a third basis for liability, inducement, under which software developers could be held liable for secondary infringement if they "induced" the use of their software to commit copyright infringement.[49]

The Court created one important exception for secondary copyright liability. In *Sony Corporation v. Universal City Studios*, 464 U.S. 417 (1984), the Court held that contributory liability for copyright infringement did not apply to the makers of a device if that device had "substantial non-infringing use[.]"[50] The Court protected Sony from liability for producing and selling the Betamax video recording device, which permitted both time-shifting of television programs and the assembly of home libraries of television shows. This, of course, amounted to a decision not to prohibit the video recorder, because it was more beneficial than harmful for society. We are all fortunate that the Court was as open-minded as it was.

---

ed. May 14, 1998) (statement of Sen. Ashcroft). Ashcroft pushed for an amendment to ensure that the statute did not require technology to be designed in compliance with any protection measures. *Id.*

46. The Broadcast bill directly realizes Ashcroft's fear of mandating technology design to enforce compliance. *See generally* Electronic Frontier Foundation, Broadcast Flag, http://www.eff.org/IP/broadcastflag (last visited Feb. 9, 2007); Public Knowledge, Broadcast Flag, http://www.publicknowledge.org/issues/broadcastflag (last visited Feb. 9, 2007).

47. *See, e.g.*, *Sony*, 464 U.S. at 487 (citing Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

48. *See, e.g.*, *Napster*, 239 F.3d at 1022 (9th Cir. 2001) (citing *Gershwin Publ'g Corp.*, 443 F.2d at 1162).

49. *Grokster*, 545 U.S. at 936-38.

50. *Sony*, 464 U.S. at 442.

E. Innovations Under Attack

1. Peer-to-Peer Filesharing

One of the most controversial innovations in recent years has been software for peer-to-peer filesharing, often known as P2P. P2P networks allow individuals to exchange digital files with other computers connected to the Internet. Users can download copies of files offered by others, and can upload their own files to the network. Most networks enable users to search for files that match a user-entered description. These networks are commonly used to exchange copyrighted digital media files, such as music and movies. The copyright holders have used the legal system to challenge both the distribution and the use of P2P software programs.[51]

The first major peer-to-peer network was Napster. The Napster system consisted of a central index that linked to files offered by users; this central index enabled participants in the system to quickly locate desired content.[52] Multimedia content producers quickly brought suit against the software developers to prevent the continued operation of the network and distribution of the software. The Napster creators lost these suits, the Napster server was shut down, and the software distributors stopped development and distribution. Grokster, a peer-to-peer file sharing network that operates without a central index, succeeded Napster.[53] Content producers brought suit again, to hold the developers liable for the copyright violations of the users of the software.[54] Future peer-to-peer filesharing networks, more technologically advanced and more difficult to shut down than Grokster, will no doubt lead to more lawsuits.[55] In addition to suing the innovators, the content producers are

---

51. *See BMG Music*, 430 F.3d at 888; *Napster*, 284 F.3d at 1091.

52. *Napster*, 239 F.3d at 1011-12. Since its legal challenge, the Napster name and logo have been assigned to a legal music download-for-pay service. *See* Napster, http://www.napster.com (last visited Feb. 9, 2007).

53. *See Grokster*, 545 U.S. at 919-27 (describing Grokster's architecture).

54. The suit reached the Supreme Court in *Grokster*, in which the Supreme Court held that secondary liability for copyright could be triggered by "inducing" direct infringements of copyright; the Court then remanded the case for further proceedings considering liability under this theory. *Id.* at 936-38.

55. The Freenet and BitTorrent represent different technological advancements beyond the Grokster network. Freenet adds redundancy and anonymity to strengthen peer-to-peer networks against disruptions. Freenet Project, http://freenetproject.org (last visited Feb. 9, 2007). BitTorrent breaks large files into small pieces and uses multiple sources for each download. BitTorrent, http://www.bittorrent.com (last visited Feb. 9, 2007). This makes BitTorrent the technology of choice for downloading pirated movies, along with legitimate large digital. The MPAA has been very resistant to BitTorrent, and many popular "trackers" (sites providing pointers to file downloads), including the once-popular LokiTorrent, have settled. Ashlee Vance, *MPAA closes Loki*, REGISTER, Feb. 10, 2005, http://www.theregister.co.uk/2005/02/10/loki_down_mpaa/.

also suing the users of the networks for direct copyright infringement.[56] Because the targets of such suits cannot afford to risk full liability (where a damage award could amount to $150,000 per song),[57] the vast majority have settled out of court.[58]

Peer-to-peer filesharing may well have considerable negative effects, beginning with the narrow economic effects focused on reduced sales by music producers. It is quite rational to assume that many consumers will not purchase music that they can acquire in a nearly identical form for free. As the corporation loses more money, it receives less in return for its investments in the artists and in production, marketing, and distribution. This may discourage some individuals from starting recording companies, and may lessen expansion efforts of existing companies, possibly depressing the entire industry. Many skeptics have responded by claiming that the actual losses caused by peer-to-peer file sharing are nowhere near as large as alleged[59]; some note that music sharing exposes users to many new bands, supplementing the marketing efforts of the recording industry, and thus results in increased sales.[60] But we cannot determine with any degree of certainty how much money recording companies are losing because of file sharing; we certainly cannot tell how much they would lose if the legal system were to condone file sharing. It is possible that a great many more music fans would acquire their music for free.

However, punishing the file sharer and punishing the software developer are not the same, even if they are intended to address the same problem. Punishing the software developer harms society in other ways which must be taken into account. Peer-to-peer networks, especially modern ones such as BitTorrent, are efficient means of distribution for digital content.[61] They greatly reduce unnecessary overhead in production and distribution, not just for music files, but also for large software packages and other files.[62] BitTorrent technology is currently used to transfer many legal files.[63] If the BitTorrent software were

56. *See BMG Music*, 430 F.3d at 888.

57. 17 U.S.C. § 504(c)(2) (2000).

58. *See, e.g.*, *Court Rules Against Song Swappers*, BBC NEWS, Jan. 27, 2006, http://news.bbc.co.uk/2/hi/entertainment/4653662.stm; *but see BMG Music*, 430 F.3d at 888.

59. *See, e.g.*, Michael Geist, *Piercing the Peer-to-Peer Myths: An Examination of the Canadian Experience*, FIRST MONDAY, Apr. 2005, http://www.firstmonday.org/issues/issue10_4/geist/.

60. *See, e.g.*, Owen Gibson, *Online File Sharers 'Buy More Music'*, GUARDIAN UNLIMITED, July 27, 2005, http://www.guardian.co.uk/arts/news/story/0,11711,1536886,00.html.

61. *See, e.g.*, John Borland, *File Swapping Shifts Up a Gear*, CNET NEWS.COM, May 27, 2003, http://news.com.com/2100-1026_3-1009742.html.

62. *Id.*

63. New versions of the Linux operating system are routinely distributed through BitTorrent, as they are downloaded by many users in parallel shortly after their release. *See,*

prohibited, society would lose the benefit of using the network for these transfers. And this loss is insignificant compared to the chilling effects that would follow from punishing the developers of the networks. Punishing the developers might scare away the programmers who would otherwise have developed the software behind the next revolution.

2. Blizzard v. BnetD

The recent 8th Circuit Case *Davidson & Associates, Inc. v. Internet Gateway*, 422 F.3d 630 (8th Cir. 2005), also known as "Blizzard v. BnetD," concerns the video game company Blizzard's "Battle.net" online service, which enables users of multiple Blizzard video games to play each other over the Internet.[64] As part of its functionality, the Battle.net service prevented pirated copies of the video games from being played online.[65] Out of frustration over problems with the service, a group of users of Blizzard games developed their own server software, "BnetD," to replace Blizzard's official servers.[66] The BnetD designers could not enable their server to block illegal games, as Blizzard did not make available its detection process for illegal games.[67]

Blizzard brought suit against the BnetD designers in order to enjoin the operation of their service, alleging violations of the Digital Millennium Copyright Act and of the license agreements for use of the software.[68] The programmers of BnetD in response claimed that their actions in creating the BnetD service constituted reverse engineering to produce an interoperable product, and thus were covered by explicit protections for reverse engineering in the DMCA.[69] But because BnetD-

e.g., The Linux Mirror Project, http://www.tlm-project.org (last visited Feb. 9, 2007).

64. Full details on the case, including links to all court documents, are available through the Electronic Frontier Foundation, who served as co-counsel for the case. Electronic Frontier Foundation, Blizzard v. BNETD, http://www.eff.org/IP/Emulation/Blizzard_v_bnetd (last visited Feb. 9, 2007). The district court decision found for the video game manufacturers. *See, e.g.*, Davidson & Assoc., Inc. v. Internet Gateway, Inc. (Internet Gateway I), 334 F. Supp. 2d 1164 (E.D. Mo. 2004).

65. Brief of Defendants-Appellants at 17, Internet Gateway II, 422 F.3d 630 (8th Cir. 2005) (No. 04-3654).

66. *Id.* at 8.

67. Given the weakness of the authentication mechanism, widely publishing this information would have made it easy for users of unauthorized copies of the games to disguise their games as legitimate. This is known in the computer science community as "security through obscurity," and is considered unacceptably weak. *See, e.g.*, S. Forrest et al., *Building Diverse Computer Systems*, 1997 PROC. OF THE 6TH WORKSHOP ON HOT TOPICS IN OPERATING SYS. 71 (1997) ("Within computer security there is widespread distrust of 'security through obscurity' . . . .").

68. *Internet Gateway I*, 334 F.Supp. 2d at 1167.

69. *Id.* at 1183-84. The DMCA's protections for reverse engineering are codified at 17 U.S.C. § 1201(f) (2000). The parties' argument was based on a recent case upholding this exception in the context of reverse engineering printer ink cartridges. *See Lexmark Int'l*, 387 F.3d at 522.

based servers permitted illegal copies of games to be played online, the district court found that the actions of the BnetD developers went beyond the scope of the exception for production of interoperable products and constituted copyright infringement.[70] Additionally, the district court found that the BnetD program constituted an anti-circumvention device in the language of the DMCA.[71] The Eighth Circuit affirmed the judgments of the district court.[72]

Permitting the BnetD server to operate bears little risk of significant social harm. There are two categories of possible damages: competition between BnetD and Battle.net, and the marginal increase in the value of illegal copies of Blizzard games (coupled with a greater incentive to make such copies) through online play enabled by the use of BnetD-based servers. As for the former, if the BnetD server is good enough to take users away from the (free) Battle.net service, then it possesses inherent social value which exceeds the minor loss in Blizzard's motivation to invest in the service resulting from the lost advertising revenue associated with the service. Additionally, if Blizzard improves their Battle.net service to win customers back, society benefits from the competition.

As for the marginal increase in value of illegal games, it is possible that Blizzard may lose some sales revenue. Some who would otherwise have bought a legal copy of a Blizzard game may decide to acquire an illegal copy because the BnetD server permits the illegal copy to be played online. But this is a small portion of the value of the video games – even without the Battle.net server, illegal copies of games can be played offline, and even over Local Area Networks (LANs). As a method for discouraging piracy, reducing the value of the games by this small a margin is likely to prove ineffective.

Prohibiting the BnetD server, on the other hand, carries a great risk of significant social harm. It grants Blizzard the power to eliminate any competition with their Battle.net service. While the court did not grant a damage award to the plaintiffs, as that issue was settled out of court,[73] an award of damages in a similar case would have the same chilling effects discussed in the context of peer-to-peer networks. Additionally, the 8th Circuit upheld in full the software license agreement governing the Blizzard software, despite its conflict with the reverse engineering protections of the DMCA.[74] This decision ignores a Congressional balance governing technological protection measures, and it may have

70. *Internet Gateway I*, 334 F.Supp. 2d at 1184-85.
71. *Id.* at 1186-87.
72. *See Internet Gateway II*, 422 F.3d at 630.
73. *Internet Gateway I*, 334 F. Supp. 2d at 1167.
74. *Internet Gateway II*, 422 F.3d at 641-42.

repercussions which extend far beyond this case and which cause great detriment to society.[75]

3. Tor

The Tor communications system is an implementation of a technology known as "onion routing."[76] Onion routing protects the anonymity of an Internet user by routing messages through multiple intermediate nodes.[77] Each intermediate node hides the origin of messages in such a way that a reply message can reach the original source node, and yet no node knows more of the path of the message than the nodes immediately before and after it on the message path.[78]

Providing anonymity for Internet traffic has significant positive social benefits. The anonymity and encryption provided by the service make it far more difficult for ISPs and nations to censor the speech of Internet users, and make it impossible to monitor Internet traffic to collect personal information. But anonymizers, like Tor, enable undesirable activities as well. Users of the Tor network can transfer copyrighted files or child pornography through the network. Anonymity makes it more difficult for law enforcement officials to determine the identity of the illegal actors.

The legal status of Tor is far from clear. Because Tor can be used to facilitate the transfer of copyrighted files without detection, the governing legal doctrine is secondary copyright infringement. The tests of *Sony* and *Grokster* apply. The rule of *Sony* is that contributory liability for copyright infringement cannot be assigned to the makers of a device if that device had "substantial non-infringing use[.]"[79] Tor clearly has some non-copyright-infringing uses, through its protections of free speech and privacy. Whether this is "substantial" is a decision for the courts to make. The *Grokster* opinion holds that the makers of a device can be held liable for secondary infringement if they "induced" the use of the device in an infringing manner.[80] This opinion has not been widely tested, and it is unclear what will constitute inducement, and unclear whether or not this doctrine could be used to regulate Tor.

As with other innovations, the positive social value of the Tor network is significant, and must be considered even if the system

75. This was one of the primary arguments of the counsel for the defendants. Brief of Defendants-Appellants, *supra* note 65, at 39.

76. Tor Homepage, http://tor.eff.org/ (containing a basic description of the Tor system and onion routing technology) (last visited Feb. 10, 2007).

77. Tor, Overview, http://tor.eff.org/overview (last visited, Feb. 10, 2007).

78. *Id.*

79. *Sony*, 464 U.S. at 442.

80. *Grokster*, 545 U.S. at 936-38.

facilitates illegal activity.

4. Google Book Search

The Google Book Search project allows users to search for keywords and phrases in digitized versions of books.[81] The service acquires books from two sources – publishers provide books directly to Google, and libraries loan books to Google to be scanned (and then returned).[82] Google makes this information available to three different extents. If a book is out of copyright, Google permits the user to scan the entire book. With permission from the publisher or author, Google allows a few sample pages of the book to be seen.[83] Otherwise, Google displays card catalog information about the book, and a few sentences around the search term.

The structure of this system provides the most benefit to users while causing the least harm to the interests of the copyright holders.[84] As with many of its products, Google has deliberately chosen not to internalize many of the benefits of the service.[85] This service is an enormous public good and does little harm to publishers. It may in fact benefit them extraordinarily, as it makes it easier for consumers to find books they may want to purchase. Despite all of this, many otherwise innovation-friendly thinkers have spoken out against the project.[86] Two lawsuits have already been filed against Google by groups of publishers.[87] Their suits are not unfounded – Google's actions include making an

81. Google, About Google Book Search, http://books.google.com/intl/en/googlebooks/about.html (last visited Feb. 10, 2007).

82. *Id.*

83. *Id.* Note that the Google site says "publisher or author", but depending on the author's agreement, it is likely that a published book would require the publisher to agree to the display.

84. *See* Eric Schmidt, Op-Ed, *Books of Revelation*, WALL ST. J., Oct. 18, 2005, at A18; Posting of Susan Wojcicki to Official Google Blog, http://googleblog.blogspot.com/2005/09/google-print-and-authors-guild.html (Sept. 20, 2005).

85. Schmidt, *supra* note 84 ("[W]e don't make a penny on referrals. We also don't place ads on Google Print pages for books from our Library Project, and we do so for books in our Publishing Program only with the permission of publishers. . . .").

86. Posting of Siva Vaidhyanathan to Sivacracy.net, http://www.nyu.edu/classes/siva/archives/001841.html (Aug. 12, 2005) (saying that Google's actions may lead to a "copyright meltdown", in which publishers will request and receive Congressional support in further tightening their copyrights). *But see* Posting of Derek Slater to A Copyfighter's Musings Blog, http://blogs.law.harvard.edu/cmusings/2005/10/24#a1449 (Oct. 24, 2005).

87. One suit pits the Author's Guild against Google. Complaint, Author's Guild v. Google Inc., No. 05-CV-8136 (S.D.N.Y. Sep. 20, 2005), *available at* http://news.findlaw.com/hdocs/docs/google/aggoog92005cmp.pdf. The other suit pits McGraw-Hill and other publishers against Google. Complaint, McGraw-Hill Cos. v. Google Inc., No. 05-CV-8881 (S.D.N.Y. Oct. 19, 2005), *available at* http://www.publishers.org/press/pdf/40%20McGraw-Hill%20v.%20Google.pdf.

unauthorized (digital) copy of the published works, though Google has a credible fair use defense.[88] While it would be better for Google to obtain permission from publishers before digitizing their works, this is simply not feasible given the transactional (and actual) costs of negotiating with every publisher over every work. As James DeLong puts it, "[t]o insist that Google get permission means that the post-1923 literature cannot be included."[89]

Google Book Search is different from the preceding examples in many ways. For one, it is the innovation of a major (and wealthy) American corporation. This means that Google is not judgment-proof – it could be held liable for immense damages. At the same time, Google's history of valuable innovations and of being "good"[90] have not gone unnoticed by the public. The risk of losing Google's innovations is far more cognizable than the risk of losing the innovations of an unknown amateur programmer.[91] For another, this is not an innovation in the same sense as others. This is not a single new software program, such as a file sharing client or a network routing tool. But Google Book Search is very much a new software innovation, in part because it represents a new combination and use of existing software tools, and in part because it creates new beneficial and harmful activities that need to be balanced to determine the overall social equity of the service. The Google Book Search example highlights the tradeoff that innovation policy is intended to resolve – it is a software innovation that creates massive social benefits, yet it violates the law as it is constructed. The primary question, then, is whether the violation is so egregious as to require the service to be stopped, or whether the social benefits outweigh the harms.

---

88. Google's claim to fair use may rest in its efforts to transform (by digitizing) the copyrighted work, that it does not overly harm the market for the work, and that it results in significant social value. *See* Kelly v. Arriba Soft Corp., 77 F. Supp. 2d 1116, 1118-23 (C.D. Cal. 1999), *aff'd in part, rev'd in part*, 336 F.3d 811 (9th Cir. 2003); Siva Vaidhyanathan, *A Risky Gamble With Google*, CHRON. OF HIGHER EDUC., Dec. 2, 2005, at B7, *available at* http://chronicle.com/weekly/v52/i15/15b00701.htm; Posting of C.E. Petit to Scrivener's Error, http://scrivenerserror.blogspot.com/2005/10/authors-guild-v-google-5-fair-use.html (Oct. 4, 2005).

89. Posting of James DeLong to IPCentral Weblog, http://weblog.ipcentral.info/archives/2005/10/the_google_prin_1.html (Oct. 20, 2005).

90. Google, Our Philosophy, http://www.google.com/intl/en/corporate/tenthings.html (last visited Feb. 10, 2007) (referring to Rule #6, "[y]ou can make money without doing evil").

91. As Derek Slater puts it, this may be "a chance for a legitimate defendant to take a real shot at making some good law." Slater, *supra* note 86.

III. WHAT IS PROPER SOFTWARE INNOVATION POLICY?

A. Grokster*, or: What is Improper Software Innovation Policy?*

The Supreme Court in *MGM v. Grokster* delivered the most recent statement on software regulation.[92] Before the court were many strong arguments supporting the Grokster software. Respondents' brief notes many values of the technology developed by Grokster. It improves reliability and efficiency over related programs.[93] Businesses have developed around use of the technology.[94] Many music artists have supported the technology, recognizing that it improves their name recognition and increases their fanbase.[95] Respondents also note that, given their originality, the technical innovations may lead to unforeseen future value.[96] Furthermore, the respondents note that any decision to regulate the innovation may lead to complex and expensive future litigation to determine the limits of valid technologies.[97] All of these factors are significant in determining whether as a matter of policy a technology innovation should be regulated.

Justice Breyer's concurrence addresses some issues of the benefits and harms of innovation. Breyer emphasizes *Sony*'s explicit balance of interests,[98] enumerates many positive values of digital technologies,[99] and even considers the respondents' concerns that updating the technology to add a filtering mechanism may be prohibitively difficult[100] and that the technology has led to many new valuable, legitimate businesses.[101]

The majority opinion, in contrast, did little to protect the benefits of innovation. It acknowledged the technical benefits of the innovation and the value of non-infringing uses of the technology.[102] It also expressed a concern that the wrong legal standard may have negative repercussions on legitimate innovation.[103] The Court left *Sony* intact (though still unclear), and it adopted an "inducement" theory of liability, to separate

---

92. *See,* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

93. Brief for Respondents at 6-8, *Grokster*, 545 U.S. 913 (No. 04-480).

94. *Id.* at 21.

95. Jonathan Krim, *Artists Break with Industry on File Sharing*, WASH. POST, Mar. 1, 2005, at E5.

96. Brief for Respondents, *supra* note 93, at 25.

97. *Id.* at 30-31.

98. *Grokster*, 545 U.S. at 949-50 (Breyer, J., concurring).

99. *Id.* at 950-56 (Breyer, J., concurring).

100. *Id.* at 957-59 (Breyer, J., concurring).

101. *Id.* at 963-65 (Breyer, J., concurring).

102. *Id.* at 919-20.

103. *Id.* at 936-37. ("We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential.").

out and hold liable those developers who acted to induce others to directly infringe copyright, independent of any other grounds for liability.[104] This move further protects the interests of copyright holders, and further chills innovation, to the detriment of society.

Inducement and the existing doctrines of contributory and vicarious liability form a three-part test for liability (with one important exemption). The three parts of *Grokster*'s liability test are all directed primarily to the software's developer.[105] As a proxy for determining whether the software itself is worth protecting, secondary liability investigates the motive, knowledge, and ongoing activity of the software's developer. The Court modified the secondary liability doctrine through *Sony*, creating a technology-specific exemption for devices which have "substantial non-infringing use."[106] This safe harbor restores some of the balance by protecting devices which already have beneficial social value. But even in its original conception, its attachment to static, demonstrable positive uses limits it, given the dynamic nature of the equity of uses of software discussed earlier. And the Supreme Court in *Grokster* emphasized that the exception applies only to contributory copyright liability, and in particular, does not provide an exception to liability for inducement. Even beyond these limitations, the flaws with *Grokster* run deeper than questions of scope. Determining liability for software development on the basis of the activities and motives of developers can produce only an approximation of correct policy because it looks solely at peripheral factors that often bear little relation to the actual social value and harm of the software.

So why persist in the illusion? In part, because it is far easier to create bright-line rules judging human conduct than to create clear rules for the proper social balance of the benefits and harms of technology. One of the foremost concerns of innovation policy is for chilling effects, and establishing bright-line rules (regardless of their correctness) helps developers know how they can avoid liability. Even if an ad-hoc standard based on the value of the technology made more correct decisions, it might be worse for innovation if every developer feared facing and losing a judgment.

---

104. *Grokster*, 545 U.S. at 936-37.

105. Inducement liability examines only the conduct of the actor – whether the actor has promoted the use of the software for infringing purposes. *Id.* Vicarious liability questions the relationship of the developer to the software, in particular whether the developer has the ability and duty to police uses of the software for infringing purposes. *Id.* at 930 n.9. Contributory liability considers in part the technology in requiring "material contribution" to the infringement. *Napster*, 239 F.3d at 1022. But an equal part of the test is the question of whether the actor has knowledge of the infringing activity. *Id.* at 1019 (citing *Gershwin Publ'g*, 443 F.2d at 1162).

106. *Sony*, 464 U.S. at 442.

In theory, this is a strong argument. But comments on the *Grokster* decision have emphasized that it is highly ambiguous.[107] Not only did the Court fail to resolve existing ambiguities in the interpretation of the *Sony* standard,[108] but it also created additional ambiguity by adding a theory of liability based on the intent of the developer.[109] Considerations of intent can be valuable for proper innovation policy, but in the inducement theory as introduced by the *Grokster* court, they both worsen the law's clarity and more strongly attach liability to the actor (and not the software itself). Additionally, the evidentiary requirements for determining the developer's intent will require many cases to survive summary judgment, increasing the risk of expensive litigation and increasing chilling effects imposed on other developers.

B. Separating Liability from Remedy; Separating the Technology from the Developer

Software innovation policy must balance the benefits of individual software innovations, the legal entitlements they harm, and the repercussions of assigning or not assigning liability. It must not prohibit software too readily, or too many social benefits will be shut off. It also must not construct remedies in a manner that places excessive chilling effects on other software developers. Proper policy separates the question of liability for the development and distribution of software into two questions, one of (pure) liability and one of remedy. The liability question focuses on the technology itself, on its benefits and harms to society. The remedy question, asked only if liability is found, focuses on the developer and on the incentives created by assigning various forms of punishment. Current law conflates and misdirects these questions, and as a result, delivers incorrect results. By separating these questions, courts can make optimal dynamic balances while avoiding unnecessary litigation expenses, preserving as much clarity of law as is feasible, and minimizing chilling effects imposed on other developers.

---

107. *See, e.g.,* Galen Hancock, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.: Inducing Infringement and Secondary Copyright Liability*, 21 BERKELEY TECH. L.J. 189, 189 (2006) ("At the same time, Grokster may frustrate copyright owners who will have to satisfy a new and ambiguous indirect infringement standard."); Jefferson Graham, *Entertainment Firms Win File-Sharing Duel*, USA TODAY, June 27, 2005, *available at* http://www.usatoday.com/tech/news/techpolicy/2005-06-27-fileshare-cover-usat_x.htm ("Chipmaker Intel, which filed legal documents in support of Grokster, said the ruling was so ambiguous that the company didn't have an immediate reaction.").

108. *See, e.g.*, Evan F. Fitts, Note, *Inducement Liability for Copyright Infringement is Born*, 71 MO. L. REV. 767, 782 (2006) ("The Court's failure to remedy the ambiguous standards set forth in Sony could have negative effects.").

109. On some level, of course, intent is also a factor in other theories of liability. But it is more central to inducement, which asks if the objective of the developer was to promote the use of the software by others for infringing purposes.

1. The Liability Rule

The question of liability for a software program is, at its heart, the question answered by the court in *Sony*. If technology has both benefits and harms, at what point can a court (or legislature, for that matter) say that the benefits exceed the harms and the technology should not be prohibited? The *Sony* court famously answered this question by declaring that a technology developer could not be liable for contributory copyright infringement if the technology has "substantial non-infringing use." This is a good start for proper policy, but it is too limited. It is limited in its legal applicability, as its safe harbor does not protect against other forms of secondary liability. It is also limited in its scope of consideration, as it reaches only a static balance of interests – current uses, both beneficial and harmful.

The proper rule for determining liability begins with *Sony*'s examination of beneficial and harmful current uses of the technology. It then considers foreseeable future uses of the technology – considering not just empirical reports of current usage patterns, but also trends in usage patterns and expert testimony as to future uses of the technology. Most importantly, the rule weighs the costs of avoiding the harms and retaining the benefits, whether these costs are incurred by the innovator or by the incumbent rights holder.[110] If the innovator can cheaply avoid or reduce the harms of the technology, then a court should favor a finding of liability, to provide an incentive for the innovator to incur the expense of the modifications. Conversely, if the harms can be easily mitigated or avoided entirely by the incumbent rights holder, this should go far towards a finding of no liability.

To avoid the harms, the innovator can modify the technology, for example, by adding filters to a filesharing program to block transfer of copyrighted works. This generates two costs: the cost of implementing the modifications, and the damage that the modifications have on the beneficial uses of the technology, such as false positives generated by a filtering technology, or a heavy burden of additional user effort (such as needing to verify legitimate files) that discourages adoption of the technology. The incumbent rights holder can forestall or at least mitigate the harms as well, through a wide variety of mechanisms. Sometimes the rights holder may be able to increase technological protection measures governing the technology.[111] Some measures are more expensive to implement, such as designing an online distribution system like Apple's iTunes to compete with the filesharing systems, but these systems can

110. This is reminiscent of the "cheapest cost avoider" theory of tort law, and for good reason.

111. Though, this can lead to inefficient racing behavior, if the new modifications can be easily compromised.

also result in great increases in revenue for the company and great benefits for society as a whole.[112] These changes incur costs for implementation and for reductions of the benefits of the innovation, as before. As the example of iTunes demonstrates, they also have the potential to result in broader social benefits; while these are highly speculative, to the extent they can be foreseen, they should also be included in the balance.

Critics of my approach will note that it is on some level more restrictive than the balance drawn by *Sony*. While this approach more clearly acknowledges many of the external costs of regulating or permitting an innovation, it is not as permissive of speculative future benefits as the Court's standard in *Sony*. By permitting any technology that has "substantial non-infringing use," many interpret the *Sony* rule as leaving room to protect innovations that may in the future have significant beneficial use, even if that use is not immediately foreseeable. The rule I offer deliberately omits this consideration, for two reasons. First, while innovations do sometimes lead to unpredictable significant benefits, these are highly speculative and unlikely (in particular if they're not at all foreseeable *ex ante*), and it seems unfair for them to outweigh demonstrable, significant harm in the present. Second, it is also possible that the innovations will lead to significant unforeseeable harms – this is, after all, the nature of the unforeseeable. Any policy must make some compromise, and it is just too costly to permit a current harm out of a purely speculative possibility of future benefits.

2. The Remedy Rule

Once an innovation has been found to be against society's best interests, the next question concerns the proper response. The weaker response merely enjoins the continued distribution and development of the software. The stronger response holds the developer liable for damages. The current legal system takes the latter approach, subjecting secondary infringers to considerable damages.[113] These damages serve

112. *See* Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002) (the approach of "creative destruction" at work).

113. Secondary copyright infringement imposes the same liability as direct infringement, which carries large statutory damage awards. In practice, the parties often settle on a considerably smaller sum of money, along with injunctive relief. *Compare* How the RIAA Litigation Process Works, http://info.riaalawsuits.us/howriaa.htm#set (last visited Mar. 27, 2007) ("settlement is usually for $3750, non-negotiable, and contains numerous one-sided and unusual provisions, such as a representation that peer to peer file sharing of copyrighted music is a copyright infringement"), *with* 17 U.S.C. § 504(c)(1)-(2) (2000) (authorizing "not less than $750 or more than $30,000" for each infringed work, or up to $150,000 if the copyright owner demonstrated that the infringement was willful).

as a considerable incentive to discourage others from infringing in the future. But these incentives can become too severe. Holding an innocent developer – one who did not intend or desire that his product be used for copyright infringement – liable for large damages scares other innocent developers, who will fear that their products will be wrongly used by others, subjecting them to large damages, placing their personal assets at risk. Instead of indiscriminately imposing damages, a court can apply an intent-based standard in awarding punitive damages, thereby limiting the liability of innocent developers that simply distribute and develop the software.

The Supreme Court has laid the groundwork for such a distinction in its inducement theory in *Grokster*.[114] The Court did not specify the amount of encouragement necessary to trigger liability; many cases will likely be decided to resolve the right threshold. The bar must be set high to avoid assigning large damages to innocent actors. One appropriate standard would be to assign damages only if no reasonable person could interpret the actions of the innovator to be in good faith and without redeeming social value; this standard, resembling that of criminal law, would go far towards eliminating the worst chilling effects imposed on software developers.

C. The Difference Between a Liability/Remedy Test and Grokster

As we have seen, elements of the existing standards of *Sony* and *Grokster* can be key components to a proper standard. But as it is currently constructed, the standard of *Grokster* both over- and under-protects innovation. Because it places so much emphasis for its liability on the intent of the developer, it will find many harmless (and even beneficial) programs liable. Less obvious is the standard's risk of underprotection. It is possible for a software program developed by an innocent developer to fail a balance of interests test, even if the developer has no intention of enabling illegal use. Both of these errors are not simply problems of execution where the standards of *Grokster* are valid but simply applied too tightly. They are deep, fundamental problems with the approach of all existing cases concerning innovation regulation.

1. Overprotection – The NES Emulator

As mentioned above, *Grokster* overprotects when it assigns an inappropriate remedy – assigning damages in circumstances where they serve perverse incentives. But *Grokster* also overprotects at the liability

114. Though the court in *Grokster* introduced inducement as a theory of liability, its principles apply to this context as well.

stage, as it prohibits innovations that were intended to break the law but are, on balance, beneficial for society. This includes, for example, technologies which were created for nefarious purposes and can be readily thwarted. An example would be an easily filtered communications program, designed to exchange illegal files, that also allows for the efficient transfer of other types of files. More importantly, it includes technologies where the harm is significant from a legal perspective but negligible from a practical perspective.

Consider a Nintendo Entertainment System ("NES") emulator.[115] This emulator assists individuals who copy digital files of NES cartridges by enabling them to play the games. It also creates considerable value by enabling additional uses of the video games, uses not contemplated by the games creators. How would the *Grokster* standard treat the NES emulator? Suppose the developer openly intended and encouraged the use of the emulator with unlicensed copies of NES games. It seems certain that a court would find the developer liable for contributory infringement – the software enables the play of copyrighted games, clearly contributing to infringement, and the developer's demonstrable intent is certainly enough to constitute knowledge. The *Sony* safe harbor may or may not protect the developer – it would depend on the court's analysis of the legality of an owner of the game's use of the emulator to play a digitized version of the game, and on the court's empirical determination about the percentage of these uses. Vicarious liability likely would not apply, as the developer released the software without any retained control. Ultimately, though, a court would find the developer liable under inducement theory, as the stated intent of the developer was to enable and encourage infringing use.

Innovation policy would answer the question of liability in the reverse. The NES emulator passes both static and dynamic components of a balance of interests test. Its harm to current interests is miniscule. Aged systems such as the original NES have insignificant markets – the video game industry is characterized by a particularly short shelf life, and a decade after a system is released, it is worthless. Furthermore, any additional sales do not contribute anything to the copyright holders, as all transactions take place in used video game stores and through online sales by private individuals. Beyond these limitations, the benefits of the software are considerable. Players of the games no longer need to struggle with old, malfunctioning hardware; players who value the games at less than their purchase price can play and enjoy the games; and all

115. An emulator is a software program that mimics the functionality of a physical console. It can execute the digital code of the original video game file, translating keyboard keys into joystick commands and translating television output into screen output. Wikipedia, Console Emulator, http://en.wikipedia.org/wiki/Console_emulator (last visited Mar. 27, 2007).

players can install the emulators and games on laptops to play while traveling, an activity not possible using the original consoles.[116] The only static harm caused by the emulators is to those who would resell their physical games – but there is significant nostalgic value in the physical games and systems, value which far exceeds the value of the games themselves.[117]

The dynamic balance of interests reinforces this. Potential buyers of systems may be discouraged from making a purchase, knowing that they will eventually be able to play the games through emulators; as a result, sellers may be harmed by the lost volume. But we are considering here only emulators of systems which are long past their prime – say, at least a decade. Few video game fans who contemplate spending $300 or more on a system and $50 on a new game will choose to wait 10 years in order to play the games for free. And overshadowing this marginal harm is the value of letting future developers play with the emulator and the games, creating new levels and modifications and brand new games with ease.[118]

2. Underprotection – PeerProduce

The standard of *Grokster* may be underprotective as applied to developers whose innovations have unintended or undesired harmful uses. There are many general-purpose innovations which have both legitimate and illegitimate potential uses, including software based on encryption, the protection of anonymity (such as Tor), file exchange (such as peer-to-peer file sharing), and DRM circumvention (permitted for reverse engineering for interoperability).[119] Some of these may be created by a developer who has no desire or even suspicion that the device can be used for illegal purposes.

Consider a hypothetical development tool, PeerProduce. PeerProduce is a tool for collaborative, distributed, peer-to-peer software development. It allows amateur programmers to share their repositories of written source code with others, and it enables others to search the network to find pieces matching the description of the software they are looking for. The search is based primarily on programmer-supplied

116. From the perspective of copyright infringement, it can be argued that none of these benefits constitute "non-infringing use" in the sense of Sony. Nevertheless, they are considerable benefits, especially measured against the limitations on the practical harm of the violations.

117. This author, in fact, is proud to own a working original NES system, along with a sizable collection of games.

118. *See, e.g.*, Mega Man vs. Ghosts 'n Goblins, http://www.brokenfunction.com/content/mmvs2/ (last visited Mar. 27, 2007).

119. More discussion is found in Part II.E above; *see also* Electronic Frontier Foundation, *supra* note 64.

descriptions of the source code they provide, but as a fallback, the search program looks at the names and folder paths of files.[120] Based on the strong organizational tendencies of software developers, PeerProduce also includes an auto-indexing feature that can take a folder full of programs and can index the folder and its subfolders to make all of the code available to and easily searchable by others. Unbeknownst to our hypothetical, naïve developer, PeerProduce can be used directly (or with some minor modifications to refine the search process) as a peer-to-peer filesharing program for music and movie files – exactly replicating the functionality of the Grokster system. PeerProduce is released without any filters on the type or contents of files or search requests.

How would the *Grokster* standard respond to PeerProduce? First, consider contributory infringement. PeerProduce certainly contributes materially to direct infringement, as it replicates the functionality of the Grokster software. Whether PeerProduce's developer knows of this assistance is a trickier question, but it is one that does not need to be resolved. This is a classic example of the *Sony* safe harbor, as the technology has substantial noninfringing use. Therefore even if contributory copyright infringement would apply, the developer would be protected by the exemption. Vicarious infringement would also exculpate the developer, who has no ability to control or supervise subsequent use of the software. Inducement liability would also not apply, as the developer had only honest intentions. None of the *Grokster* elements would apply, and continued development and distribution of the technology would be permitted.

Proper innovation policy would decide otherwise. The static balance of interests resembles that of Grokster. PeerProduce enables the exchange of copyrighted music and movie files, which (for the sake of argument) cause considerable harm to the copyright holders' economic interest.[121] It has benefits as well, of course – it greatly lowers costs of collaboration in software development, by making it easy to both offer software to others and to find software offered by others. But there are other options for this which have only marginally higher costs, such as Sourceforge, an enormous repository of open-source software.[122] The

120. For example, a searcher looking for networking software will be able to find a program containing "TCP" located in a subfolder "Net" of a folder "Utils".

121. Of course, there is much debate over this, and one could argue that the static balance of interests is in favor of PeerProduce. But, given that it is essentially identical to Grokster, this is likely not the prevailing attitude. After recognizing that "these fears [may] be offset by the different concern that imposing liability . . . could limit further development of beneficial technologies", the Court said that "[t]he argument for imposing indirect liability in this case is, however, a powerful one, given the number of infringing downloads that occur every day using StreamCast's and Grokster's software." *Grokster*, 545 U.S. at 929.

122. *See* SourceForge.net, http://sourceforge.net/ (last visited Feb. 12, 2007).

existence of these alternatives reduces the value of the software considerably. The dynamic balance of interests is mixed. Prohibiting the software from being distributed in its current form imposes some chilling effects, though far less than the effects of a large damage award.[123] Permitting the software to continue to be distributed, though, leads to greater ongoing harm to protected economic interests. Furthermore, the cost of adding filters to the system (to examine the content of the files to see if it is text/source code, or at the least to prohibit the exchange of files with an MP3 extension) is very minimal – the court can require the developer to add these to the system before it can be legally distributed.

D. Real-World Applications of the Liability/Remedy Standard

1. *Grokster*

The static balance of interests in Grokster is similar to that in PeerProduce. The harms are identical – the software enables (and is in practice used for) the transfer of copyrighted music files. The benefits of Grokster are similar, as it supports a variety of legitimate file transfer operations, including the sharing of music by artists who wish their works to be distributed through peer-to-peer networks, to increase the size of their fan-base or to distribute music that the recording label rejected. This is likely a considerably smaller share of the use of the system than the share of legitimate usage in PeerProduce. Also, as with PeerProduce, there are other options for the legitimate exchange – many artists host websites and make their music available through them – but they are not quite as effective. While the question has not entirely been resolved, it seems likely that Grokster would lose in this balancing.

On the dynamic scale, as with PeerProduce, permitting the continued distribution of the code risks ongoing harm to the copyright interests of music holders. Prohibiting the software carries the same potential chilling effects (though of course the intent test limits these by providing a high, clear standard before assigning large damages). But prohibiting the software has a different practical effect. The intended purpose of PeerProduce (the exchange of program source code) could be realized while avoiding the majority of the harms by adding simple filters for music files. Given that Grokster's primary beneficial purpose is to share music files, effective filters would need to separate authorized from unauthorized transfers, a far more difficult task. Stopping the unauthorized transfers would likely require stopping the authorized as

123. Of course, good innovation policy would not apply damages, as the harm was unintended.

well, a tradeoff that is still likely worth it, though it is a matter of debate.

As for intent and the possible assignment of damages, the Supreme Court noted, in particular, the pieces of evidence indicating that Grokster had tried to absorb as much of the former Napster user base as possible.[124] This might enough to pass some low trigger threshold, but the standard must be stricter than this, given the massive chilling effects of damage awards. Damages are not an appropriate form of remedy, without clear evidence that the developer knowingly designed the software primarily for illegal use.

2. Blizzard

In Blizzard, the harm to the copyright holder is indirect. The BnetD server allows pirated copies of Blizzard games to be played over the Internet. This produces a marginal increase in the value of pirated copies of games, and consequently a greater incentive to copyright games. But this increase is small. Even without BnetD, illegal copies of games can still be played, both offline and with friends over a Local Area Network. Also, BnetD does not share players with Blizzard – the large community of Blizzard players will still be inaccessible to those with pirated copies of games. As another type of harm, the BnetD server will draw game players away from the official Blizzard server, reducing their revenue from advertising. But to this extent, the harm is caused by competition – players with legal copies of games will only switch to BnetD if it represents a better game playing experience.[125] This is not the sort of harm that the legal system wishes to avoid. It is in fact one of the benefits of the BnetD server – it represents a competitor in the market for Blizzard video game servers, and it in fact incorporates a number of improvements.[126] Given the limitations of the harms and the strength of the benefits, a static balance of interests test would come out against regulation of the innovation.

The dynamic balance of interests reinforces this determination. Prohibiting the distribution of the BnetD server would have chilling effects greater than those of Grokster, because the creators of the server likely thought and intended that their work would be protected by the reverse engineering exceptions to the DMCA and to copyright law in general. By interpreting these exceptions narrowly so as to prohibit the

124. *Grokster*, 545 U.S. at 925.

125. Of course, if BnetD is only competitive because source code was taken from Blizzard, then it is the sort of competition that copyright law is designed to shut off. But in the actual case, and for the purposes of this hypothetical situation, questions of actual copyright infringement were not being decided. The legal question is the circumvention of a technological protection measure in violation of the DMCA.

126. Brief of Defendants-Appellants, *supra* note 65, at 4.

server, future developers will be uncertain about the legal status of any future reverse engineering activity, and on some level, uncertain about the scope of other fair use exceptions, such as the exception for educational activities. Permitting the distribution of the server, on the other hand, has considerable beneficial results. Blizzard will be forced to improve the quality of their server in order to retain players. Blizzard also may choose to share the CD-Key checking mechanism with the developers to enable them to add security measures to BnetD to prevent the use of unauthorized games.

The liability balance of interests clearly opposes regulation of the BnetD server; as a result, the question of remedy does not need to be raised.

3. Tor

The effects of Tor are considerable for both harmful and beneficial use. It is hard to weigh the benefits of free speech and privacy against the harms of child pornography and copyright infringement, and the anonymity produced by Tor protects all of these. Consider first whether the designers of Tor can modify their software to reduce the social harms. It is difficult to construct filters that can detect child pornography, but there are ongoing efforts to develop filters that can block simple transfers of copyrighted music files, and Tor does not include any such devices. It is also useful to include a blacklist – computers, identifiable perhaps by their MAC address or some other identifying information, that are not permitted to use the Tor network because they have been determined by some other means to be producers or distributors of illegal material. Given the apparent ease of including such techniques within the software, the burden of proof should lie with the Tor developers to demonstrate that these techniques are technologically unworkable, for example that their inclusion would involve a redesign of the system that would increase its latency or decrease its bandwidth and render it unable to confer its social benefits. In the absence of such a demonstration, proper innovation policy dictates that in its current form it should not be distributed or used.

The remedy rule I offer sets a high threshold for assigning large liability damages to the software's developer. Given the many beneficial uses of the Tor service, the developers must be understood to have had good intentions in producing and distributing their software, and cannot be held liable for damages. To do so would produce too many chilling effects for other software engineers who seek to promote free speech and privacy values through their tools.

4. Google Book Search

The static balance compares the direct and indirect harm to copyright owners to the benefits to consumers of the service. As Google retains a few digital copies of copyrighted works without permission, this is a clear, direct, but bounded (and small) harm. Portions of this digital copy are transmitted to consumers in search results, though Google restricts the display of this digital copy so that the amount transmitted to others is of an amount generally considered fair use.[127] Another harm is the risk that Google may leave the database insufficiently secured, enabling massive copyright violations.[128] Weighted against these harms are the benefits the service offers. For years, services such as LexisNexis have enabled scholars to search through the text of journal articles, making research considerably easier. Extending this capability to entire books will produce enormous additional benefits, sufficient to outweigh the limited and speculative harms of the service.

Many commentators have stated that, despite its size and available cash, requiring Google to gain any form of permission from every copyright owner would be prohibitively difficult.[129] As a result, requiring Google to abate the harms by requesting permission to copy the books for its own purposes would likely cause Google to abandon its efforts.[130] Though the burden of proof would lie with Google to make this demonstration, it is almost certain that it could be met, as the number of copyrighted (and orphaned) works makes this task impossible. This is not like the Tor example above – the harms and the benefits are inextricably linked, and must be taken together. And, given the relatively minor harms, the balance of equities strongly favors permitting the service to operate as is.

Given that the liability balance argues against prohibiting Google Book Search, the remedy rule need not be applied – the developers cannot be held liable for distributing a legal product.

---

127. But, of course, fair use is a multifactor test, and it is unclear whether Google Book Search is fair use. *See supra* note 88.

128. Paul Aiken, Authors Guild, Speaker at the Yale Information Society Project Conference: Regulating Search? A Symposium on Search Engines, Law, and Public Policy (Dec. 3, 2005) (one of the plaintiffs who brought suit against Google, Paul Aiken raised this point while speaking).

129. DeLong, *supra* note 89.

130. This speaks to the static balance – it's a loss of the current benefits. But in some previous examples, the decision to restrict an innovation is less harmful when examining the dynamic balance because there are simple potential modifications to avoid the harms. *See* i*nfra* Part III.D.3.

IV. CRITICISMS AND ALTERNATIVES

A. Workability

Achieving an optimal dynamic balance of interests is difficult, and creating a policy based on more than ad-hoc decision making is even more so. Many might criticize the policy proposal I have offered by saying it does not create a workable standard for courts to follow. And if the only suggestion I offered to the court was that it should look at a dynamic balance of interests instead of a static balance, this would be a legitimate concern. Courts would select a wide variety of factors to consider when crafting a dynamic balance.

But my proposal offers far more structure than that. Separating the question of liability from the question of remedy, and separating an analysis of the value of the technology from the behavior of the developer, enables courts to convert one very difficult question into two questions that are very similar to the questions of copyright law. The second question, the question of remedy, is the easier of the two. It examines the motive of the developer, distinguishing the developer whose intent was to commit infringement from the developer whose intent was innocent. This is essentially the inducement test of *Grokster* and of patent law – it is not an easy determination, but it is familiar to courts. The question of liability is somewhat more difficult, and my proposal does increase the complexity beyond that of current law, but it remains quite manageable. At its core, the balance of interests is derived from *Sony* – if the innovation has substantial beneficial (or non-infringing, in the words of the Court in *Sony*) use, then it should be permitted. This is no less workable than current law, as it is already part of the determination process. My policy proposal adds considerations of specific, reasonably foreseeable repercussions of the decision. These questions place most of the burden on the parties, who must demonstrate the repercussions of an adverse decision, ideally through expert testimony from technology professionals. Resolving such conflicts of expert opinions falls well within the bounds of ordinary judicial processes.

The policy proposal I offer cuts across existing legal systems, most of which are directed to the behavior of an actor and not to the virtues and vices of a device. As a result, it is not possible to simply adopt my approach once and for all. After all, there is no doctrine of innovation law in which to operate. This paper has primarily dealt with secondary liability for copyright infringement because in recent years this has been the active area of law. But software innovation is also heavily regulated by the Digital Millennium Copyright Act and by private contracts (particularly in the form of license agreements), as Blizzard v. BnetD

demonstrates. Software innovation policy applies whenever a software developer is brought into court for the mere creation and distribution of an innovation. The positive and negative uses of the software and the repercussions of prohibiting or permitting the software are still the key factors in the balance of interests, whether the illegal activity is measured by damage to intellectual property interests or by the violation of contract terms or by any other harm. Moreover, the dual separations of liability from remedy, and the technology from the activity of the developer, are still the right policy approach, as they help produce the optimal dynamic balance of interests and avoid peripheral chilling effects on innovation.

Perhaps proper software innovation policy will need to be integrated into existing legal doctrines over time. Or perhaps it will require legislative action, an affirmative Congressional action to protect software innovation intended to cut across other disciplines. But at the very least, judges and legislatures can consider the principles I offer as they craft legal standards across the board. They can be more cognizant of the dangers that some legal systems pose to innovation. They can also adopt separate elements of my proposal to provide some amount of support for innovation. For example, a court could apply its own liability standard, but limit awards of damages to cases where the developer demonstrably intended the innovation to be used to violate the law. In this case, the court's decision would at least avoid creating chilling effects to discourage other well-intentioned innovators.

B. Other Solutions

Many critics will reply that any solution must operate within an existing legal doctrine, and that the language of the existing statutes and broader readings of existing principles must support any policy proposals. Given that existing principles are almost universally based on static balances of interests, and that innovation policy truly cuts across legal boundaries, these limited approaches are simply not sufficient to fully protect innovation.

Much cyberlaw scholarship in recent years has focused on increasingly restrictive interpretations of intellectual property law. The stated objective of patent and copyright law is given in Article 1, Section 8 of the U.S. Constitution, in a line known by heart to many IP scholars: "The Congress shall have 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 . . . ." In the current legal climate, intellectual property law and policy are shifting towards "exclusive right" and away from "progress," treating

intellectual and digital property more and more like real property.[131] The rights of copyright holders in particular have been extended in recent years by both courts and legislatures.[132] The law contains many exceptions to these rights, such as the fair use doctrine.[133] But fair use falls far short of converting a property regime into an engine for innovation and progress. By centering the legal discussion around commercial interests, IP law ultimately fails to protect innovation.

Creative destruction is one of few theories that avoids this focus on commercial interests; in fact, it argues that society can sometimes be improved through damage to commercial interests.[134] In particular, proponents of creative destruction in cyberlaw see the traditional methods of production and distribution of cultural materials as outdated and no longer necessary.[135] Many have proposed replacing copyright law (whose purpose is to protect these outdated methods) entirely with alternate compensation methods.[136] While it might, in the long run, be efficient for society to replace copyright law (at least in the context of musical works) with an entirely different system, innovation policy must operate at a more fine-tuned level than complete regime change. Innovation policy must correctly and specifically identify which innovations are on balance beneficial and which are harmful, rather than advocating the total overthrow of existing conceptions of legal harm.

Legal scholarship also uses the First Amendment as a defense

---

131. *See* Dan Hunter, *Culture War*, 83 TEX. L. REV. 1105 (2005); Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63 (2002); Brian F. Fitzgerald, *Digital Property: The Ultimate Boundary?*, 7 ROGER WILLIAMS U. L. REV. 47 (2001). For a considerably older (but still accurate) discussion, *see* L. RAY PATTERSON & STANLEY W. LINDBERG, THE NATURE OF COPYRIGHT 213 (1991). Many have studied this transition and have offered explanations and criticisms. *See, e.g.*, Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031, 1031-32 (2005) (interpreting the increasing propertization of copyright as a transition to a state in which copyright owners internalize all of the social value of their intellectual property); Hannibal Travis, *Pirates of the Information Infrastructure: Blackstonian Copyright and the First Amendment*, 15 BERKELEY TECH. L.J. 777 (2000).

132. For a legislative example, consider the Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998) (codified as amendments to 17 U.S.C. §§ 108, 203, 301-04). Judicial action to increase copyright holders' rights has mostly taken the form of increasing grounds of liability for infringement, such as *Grokster*'s addition of inducement liability.

133. 17 U.S.C. § 107 (2000) (fair use limitation on exclusive rights in copyright).

134. *See* Ku, *supra* note 112, at 268-69 (adapting to cyber law, Schumpeter's notion of "creative destruction," in which capitalism progresses not through minor adjustments in efficiency or variety of production capabilities but through fundamental changes in economic models underlying the production).

135. *Id.* at 269 ("[D]igital technology and the Internet strike at the foundation of copyright and the industries built upon copyright by eliminating the need for firms to distribute copyrighted works and for exclusive property rights to support creation.").

136. *See, e.g.*, *id.* at 311-22; WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT (2004).

against excessive legal regulation of technology innovation and use.[137] One can rationalize the application of the freedom of speech either to expressive uses of innovations or to the expression inherent in the lines of code of tools.[138] To determine whether or not a restriction on innovation is permissible, a court could apply a variant of First Amendment doctrine to the law.[139] A court might, for example, ask whether the law is narrowly tailored to achieve a legitimate government purpose. It would examine the purpose of the law and the way in which the law was constructed, but it would not ask whether the innovation being restricted is valuable enough to be worth protecting, and it would not attempt to measure the amount of harm caused by the innovation. It would never examine the balance of value against harm. In fact, First Amendment doctrine is specifically constructed so as not to make judgments on the activity being regulated,[140] and therefore cannot serve as a guide towards proper innovation policy.

Another interpretation of the value of the First Amendment is directed less towards the speech produced and more towards the identity of the speaker. In particular, the promotion of individual speech enables the speaker to participate in democratic self-governance,[141] and promotes a democratic culture.[142] Jack Balkin goes so far as to put forth "democratic control in technological design" as one of the core values involved in the freedom of speech in the modern era.[143] This modernized conception of the freedom of speech is necessary to promote "interactivity, mass participation, and the ability to modify and transform

137. *See, e.g.*, Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Jed Rubenfeld, *The Freedom of Imagination: Copyright's Constitutionality*, 112 YALE L.J. 1 (2002); *but see* David McGowan, *Why the First Amendment Cannot Dictate Copyright Policy*, 65 U. PITT. L. REV. 281, 284 (2004) ("The First Amendment does not supply a premise a court can use to limit congressional power to give authors rights to exclude others from their works, nor to give others—including other authors—the right to use their works.").

138. *See, e.g.*, Bernstein v. U. S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996) (acknowledging that in some circumstances software code is protected speech).

139. Neil Weinstock Netanel, *Locating Copyright within the First Amendment Skein*, 54 STAN. L. REV. 1, 21-23 (2001) (proposing treating all of copyright law as a content-neutral or content-based restriction of speech, and applying First Amendment doctrine appropriately); *but see* McGowan, *supra* note 137.

140. *See* Brandenburg v. Ohio, 395 U.S. 444, 449 (1969) (overturning the clear and present danger test as used in *Whitney*, which permitted the regulation of speech which in its substance advocated violence, and establishing modern First Amendment law as neutral to the substance of speech unless its context indicates that it will result in imminent violence).

141. Outside the context of digital culture, these ideas are associated with Meiklejohn. *See* ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948).

142. *See* Balkin, *supra* note 27.

143. *Id.* at 52.

culture."[144] In the context of innovation, a democratic culture enforces a balance of power between the production industry and the individual. If users are afraid to fully use and experiment with their technology they become trapped in the role of technology consumer. This is the "passivity thesis" described in the context of copyrighted works by Michael McGowan.[145] These are interesting as cultural theories, but they serve only to offer additional rhetorical support for the statement that courts should generally disfavor assigning liability to amateur software developers. They are not capable of providing innovation policy.

None of these approaches can offer anything resembling the breadth of the proposal given in this paper. They are not comprehensive enough to protect innovation against all legal restrictions, and they are not thorough enough to consider all of the benefits and harms of innovation and the concerns of regulation. Software innovation needs and deserves a stand-alone, comprehensive policy, one that can guide judges and legislators when considering all types of legal harm.

VI. CONCLUSION

The free and open climate of technology innovation which produced the computing industry as we know it is under attack by a legal system too concerned with short-term damage to intellectual property and other corporate interests. The consequences of the actions of courts and legislatures to regulate innovation are harmful to future societies in ways that are not always obvious at first glance. The rhetoric of "piracy" and "property" sometimes drowns out all other voices. Attempts to bolster the defense of innovation by expanding exceptions to intellectual property laws or by applying some other legal regime continue to fall short. Without a clearer understanding of the dangers of restricting innovation, and without a better idea of how to structure the legal system to protect innovation without throwing all existing legal interests out the window, courts and legislators will continue to tighten the bonds on software developers.

But innovation can yet win this war. This paper proposes a stand-alone software innovation policy, a policy that protects innovation and produces the proper incentives for other actors. This balance is not hard to achieve. It can be accomplished by separating the regulation of innovation into two questions, one of liability and one of remedy. Proper policy separates the developer from the innovation, examining only the benefits and harms of the innovation when determining liability, and

144. *Id.* at 6.

145. McGowan, *supra* note 137, at 289, 323-27 (criticizing the use of this thesis to defend against copyright control of activity).

only the intent of the developer when designing the appropriate remedy. By regulating innovation this way, society can reach an optimal dynamic balance of interests, one that respects existing legal interests, discourages true bad actors, and encourages valuable innovation.

EMBRACING THE DNA FINGERPRINT ACT

PATRICK HAINES*

* Patrick Haines received his J.D. from the University of Colorado in 2007, and served as a Note and Comment Editor for the *Journal on Telecommunications & High Technology Law*. He thanks Judge Morris B. Hoffman, Judge Carlos A. Samour, Professor Philip J. Weiser, and Cynthia Sweet for their inspiration, support, and comments. Special thanks to Dr. Stefanie Krenz.

I. INTRODUCTION

The use of human deoxyribonucleic acid ("DNA") as evidence in criminal prosecutions is commonplace in this country and much of the world.[1] In addition to its use by police and prosecutors, DNA "fingerprinting" is an affordable and reliable tool of researchers in many sciences (medicine, biology, anthropology, etc.).[2] In this country, DNA evidence serves primarily to confirm the presence of identified suspects at crime scenes by matching their DNA to crime scene trace evidence.[3] In such "evidentiary use" scenarios, a suspect is compelled by warrant to provide a DNA sample after he has been identified through traditional police methods. If the suspect's DNA matches the crime scene biological evidence, the suspect's presence at the crime scene is confirmed.

The DNA fingerprints of convicted felons are currently saved in state and federal databases in accordance with state and federal law.[4] Using these databases, crime scene DNA evidence now serves a powerful "investigative use." When police find DNA evidence at a crime scene, potential suspects can be identified from the population of previously convicted felons by matching the crime scene DNA to databased DNA fingerprints. A suspect is identified when crime scene DNA matches either databased felon DNA or unknown DNA from another crime scene.[5] In this way, DNA evidence can generate suspects instead of merely confirming the presence of a known suspect at a crime scene. The match of crime scene DNA to an individual identified by his

1. *See* DNA RESOURCE, STATE DNA DATABASE LAWS: QUALIFYING OFFENSES (2003), *available at* http://www.dnaresource.info/documents/statequalifyingoffenses.pdf.

2. *See*, *e.g.*, Alan Cooper et al., *Ancient DNA: Would the Real Neandertal Please Stand Up*, 14 CURRENT BIOLOGY 431 (2004), *available at* http://download.current-biology.com/pdfs/0960-9822/PIIS0960982204003641.pdf; Yoshinori Kumazawa, *Mitochondrial DNA Sequences of Five Squamates: Phylogenetic Affiliation of Snakes*, 11 DNA RES. 137 (2004), *available at* http://dnaresearch.oxfordjournals.org/cgi/reprint/11/2/137.

3. Human Genome Project Information, DNA Forensics, http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last visited Feb. 11, 2007) [hereinafter HGP].

4. *See, e.g.*, 42 U.S.C. § 14135 (2000); CAL. PENAL CODE § 296 (West 2006); LA. REV. STAT. ANN. § 15:609 (2006); NEB. REV. STAT. § 29-4103 (2006); N.J. STAT. ANN. § 53:1-20.20 (West 2007); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2006); VA. CODE ANN. § 19.2-310.2:1 (2006).

5. *See* Press Release, U.S. Dep't of Justice, Department of Justice Announces $98 Million in Grants for President Bush's DNA Initiative and Other Crime-Solving Forensic Services (September 19, 2005), http://www.ojp.usdoj.gov/pressreleases/NIJ05048.htm. Though matching DNA from one crime scene to another does not identify suspects directly, criminal investigators report that linking investigations through DNA expands opportunities for "case breaking" evidence to be identified.

databased DNA fingerprint is known as a "cold hit."[6] Predictably, the more DNA samples in the database, the better the statistical odds of obtaining a cold hit. Adoption of a federal "sample on arrest" policy for DNA fingerprinting will dramatically expand the number of potential cold hits. The benefits of a sample-on-arrest policy, including increased generation of suspect identities and increased case clearance rates, far outweigh the potential costs of such a policy to civil liberties and individual privacy.

The DNA Fingerprinting Act of 2005 ("Act"), passed as Title X of the Violence Against Women Act Reauthorization of 2005, requires anyone arrested for any federal crime to provide a DNA sample for analysis.[7] Other federal law requires DNA samples to be collected, analyzed, and databased from individuals convicted of certain crimes, mostly violent offenses.[8] The Act requires the government to collect, analyze, and store a DNA sample from anyone ***arrested*** for any federal crime.[9] Law enforcement will benefit from the increase in cold hits which should follow the resulting growth of the DNA fingerprint sample population. Persons arrested, however, are now compelled to provide a DNA fingerprint despite being presumed innocent; these individuals will bear the costs of potential Fourth Amendment infringements and potential threats to genetic privacy.

Passage of the Act signals that DNA is transcending its original evidentiary use, where it aided in the conviction of violent felons and exonerated the wrongly convicted, and is fast becoming primarily an investigative tool. Through the Act's federal "sample on arrest" policy, law enforcement will be poised to significantly increase the number of DNA fingerprints available for cold hit matching. The question remains whether such a policy is constitutional, and though no constitutional challenges to the Act have yet reached the federal Courts of Appeals, it is almost certainly only a matter of time before the question must be decided.

This note will first summarize the background of the DNA fingerprinting debate: the history of the use of DNA evidence, the

---

6. Mark A. Rothstein & Sandra Carnahan, *Legal and Policy Issues in Expanding the Scope of Law Enforcement DNA Data Banks*, 67 BROOK. L. REV. 127, 128 (2001).

7. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 2960, 3085 (codified as amended at 42 U.S.C. § 14135a).

8. *See* 42 U.S.C.A. § 14135 (2006). The current list of federal crimes that require offender submission of DNA samples may be found at 28 C.F.R. § 28.2 (2007).

9. 42 U.S.C.A. § 14135a (2006). The same section of the Act would also allow collection of DNA samples from "non-United States persons who are detained under the authority of the United States." *Id.* § 14135a(1)(A). This language is likely directed toward PATRIOT Act detainees and is outside the scope of this casenote, but such a provision certainly deserves further consideration and analysis.

corresponding federal legislation, and the adoption of DNA "John Doe" warrants. Next, the note will identify the DNA loci used for DNA fingerprinting, describe the process of DNA sample amplification and analysis, and summarize the statistics of sample matching. The note will also consider the debate over whether DNA fingerprints contain only "junk DNA," non-coding segments that reveal no sensitive information, or whether, as some argue, DNA fingerprints contain private information.

Following this background, the note will first rebut the criticism that the use of DNA fingerprinting in criminal trials is unfairly prejudicial and tends to sway juries that have become enamored with its reputation for accuracy and reliability. The note will then introduce the two major objections to a DNA sample-on-arrest policy: first, that the threat to the constitutionally-guaranteed personal privacy of individuals is too great; and, second, that the Fourth Amendment bar against unreasonable searches and seizures should preclude involuntary DNA sampling upon arrest.[10]

The note will discuss the text of the Act as signed into law on January 5, 2006. The note will argue that the Act withstands constitutional scrutiny under either a Fourth Amendment challenge or a "penumbra" privacy rights challenge. The note aims to show that these concerns are without merit, given the nature of the DNA samples taken, the existing procedural safeguards for both sampling and sample security, and the diminished privacy rights of arrestees. In conclusion, the note will address the major objections to the Act and reemphasize the benefits of a federal "sample on arrest" statute.

II. DNA EVIDENCE: LEGISLATION, APPLICATION, AND SCIENCE

A. A Brief History of DNA Evidence Legislation

The use of DNA evidence in criminal justice began in England in mid-1980s.[11] The first reported U.S. case to admit DNA evidence came in 1988.[12] Within a decade, virtually all state and federal jurisdictions in the U.S. were admitting DNA as evidence.[13] In 1994, the Violent Crime Control and Law Enforcement Act established a federal Combined DNA Index System ("CODIS") database, but did not authorize the collection

10. U.S. CONST. amend. IV ("The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated . . . .").

11. *See generally* Alec J. Jeffreys et al., *Individual-Specific '"Fingerprints'" of Human DNA*, 316 NATURE 76 (1985).

12. Andrews v. State, 533 So.2d 841 (Fla. Dist. Ct. App. 1988).

13. 2 PAUL C. GIANELLI & EDWARD J, IMWINKELRIED, SCIENTIFIC EVIDENCE § 18-5(A) (3d ed. 1999).

of DNA samples from anyone.[14] In 1996, proposed legislation intended to facilitate CODIS sample collection failed to pass through Congress, so CODIS remained idle.[15] Finally, in 2000, CODIS began to be systematically and reliably filled with DNA fingerprint data from qualifying convicts upon the enactment of the DNA Analysis Backlog Elimination Act ("Backlog Act").[16] The Backlog Act "authorize[d] a new program of Federal assistance to States to enable them to clear their backlogs of DNA samples . . . [and to] fill a gap in the system by authorizing collection, analysis, and indexing of DNA samples from persons convicted of Federal crimes."[17]

1. Current Federal and State DNA Collection Policies

Under the Backlog Act, individuals convicted for murder, manslaughter, sexual abuse, child abuse, kidnapping, robbery, burglary, or any attempt or conspiracy to commit such crimes, would be compelled to submit a DNA sample to CODIS.[18] All fifty states followed suit, enacting their own statutes requiring criminals to provide DNA to CODIS upon conviction of a qualifying crime.[19] Later, federal legislation added all violent crimes and terrorism to the qualifying list.[20] In practice, CODIS is maintained by the Federal Bureau of Investigation ("FBI"). Federal, state and local law enforcement can input qualifying DNA samples to CODIS, and can compare locally-collected crime scene DNA to the samples collected from known individuals and from other crime scenes that are retained in CODIS.[21]

14. Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 210304, 108 Stat. 1796, 2069 (codified as amended at 42 U.S.C. § 14132 (2000 & Supp. IV 2004)).

15. *See* Pub. L. No. 104-132, § 811(a)(2), 110 Stat. 1214, 1312 (1996); Pub. L. No. 105-251 (1996).

16. DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, § 3, 114 Stat. 2726, 2728 (codified as amended at 42 U.S.C. § 14135a).

17. H.R. REP. NO. 106-900, pt. 1, at 8 (2000).

18. § 14135a (d)(1).

19. *See, e.g.*, sources cited *supra* note 4. Note that state statutes often differ from federal statutes regarding qualifying crimes. While thirty-four states have an "all felonies" policy for DNA sampling of convicts, similar to the federal policy, thirty-eight states also allow some misdemeanors to qualify. At least four states (CA, LA, TX, VA) allow sample collection upon arrest for qualifying crimes. *See* SETH AXELRAD, AM. SOC'Y OF LAW, MED. & ETHICS, SURVEY OF STATE DNA DATABASE STATUTES (2004), http://www.aslme.org/dna_04/grid/guide.pdf (last visited April 12, 2007).

20. § 14135a (d)(2). The current list of qualifying federal crimes can be found at 28 C.F.R. § 28.2 (2007).

21. § 14132.

2. An Application of DNA to Criminal Justice: "John Doe" Warrants

DNA fingerprinting has gained sufficient acceptance within the mainstream to enable legislators to amend criminal statutes in favor of its use. For example, many states have passed statutes authorizing DNA "John Doe" warrants.[22] Such warrants toll statutes of limitation, for certain felonies, when a suspect is identified solely by the DNA fingerprint left at a crime scene.[23] The DNA fingerprint is used in lieu of name, alias, or physical description to identify the accused.[24] Once the warrant is issued, the case is considered "filed" and the statute of limitations tolls.[25] Such revisions to the statutes of many states result from widespread acceptance of DNA fingerprinting as proof of identity.[26]

"John Doe" is defined as a "fictitious name used in a legal proceeding to designate a person whose identity is unknown."[27] Courts have consistently upheld DNA John Doe warrants, finding that they do not violate due process and provide adequate notice to the suspect.[28] Some states have gone so far as to revise their statutes of limitation for violent felonies such that the statutes toll automatically upon identification of a suspect by his DNA.[29]

As statutes of limitation are revised such that they toll indefinitely upon DNA identification of a suspect,[30] one wonders if the original purposes behind statutes of limitation are being ignored altogether. The Model Penal Code describes statutes of limitation as necessary to protect civil rights by assuring that prosecutions will be based on "reasonably

---

22. *See* Meredith A. Bieber, Comment, *Meeting the Statute or Beating It: Using "John Doe" Indictments Based on DNA to Meet the Statute of Limitations*, 150 U. PA. L. REV. 1079, 1089 (2002).

23. State v. Dabney, 663 N.W.2d 366, 374–75 (Wis. Ct. App. 2003) (holding that an arrest warrant which identified defendant as "John Doe" with a specific DNA profile effectively tolled the six-year statute of limitations and satisfied requirements that an arrest warrant must, if the name of the person to be arrested is not known, designate that person by any description by which that person can be identified with reasonable certainty).

24. *Id.*

25. *Id.*

26. David Doege, *Novel Warrant IDs Suspect Only by DNA Databank Evidence Used to Charge "John Doe" in Rape*, MILWAUKEE J. SENTINEL, Sept. 2, 1999, at 1.

27. BLACK'S LAW DICTIONARY 853 (8th ed. 2004).

28. *See, e.g.*, *Dabney*, 663 N.W.2d at 375 (DNA John Doe warrant did not create any lack of notice issues such as would implicate due process considerations).

29. *See, e.g.*, COLO. REV. STAT. § 16-5-401 (8)(a.5) (2006) ("[I]n any case in which the identity of the defendant is determined, in whole or in part, by patterned chemical structure of genetic information, and in which the offense has been reported to a law enforcement agency, as defined in section 26-1-114(3)(a)(III)(B), C.R.S., within ten years after the commission of the offense, there shall be no limit on the period of time during which a person may be prosecuted after the commission of the offense . . . .").

30. *See, e.g.*, § 16-5-401 (8)(a.5).

fresh evidence."[31] Statutes of limitation "provide predictability by specifying a limit beyond which there is an irrebuttable presumption that a defendant's right to a fair trial would be prejudiced."[32] Proponents of DNA John Doe warrants rebut this challenge with the argument that, unlike eyewitness testimony, DNA evidence does not lose probative value over time.[33] Additionally, DNA evidence can be independently analyzed or a match disproved by the accused, even years or decades later.[34]

But such a policy allows the State's case to stay strong, based on crime scene DNA, while non-DNA evidence (e.g., witness recollection) that may exonerate the defendant is lost over time.[35] Consequently, defendants may be prejudiced by their inability to defend against a charge kept alive through an old, stale DNA John Doe warrant.[36] Additionally, no rational argument can be made that a DNA John Doe warrant puts a suspect on notice, except where the suspect actually committed the crime.[37] This pretext, of course, violates the most fundamental tenet of American jurisprudence: innocent until proven guilty.[38] Based on these arguments, the best control on the potential abuse of DNA John Doe warrants is to ensure that they are not issued unless the probability of conviction is sufficiently high in terms of all the non-DNA parts of the case (e.g., victim availability, police availability, other corroborating evidence) to support issuing such a warrant.[39]

Much has already been written arguing the benefits and detriments of DNA John Doe warrants.[40] The practice is considered within this note only to demonstrate that DNA fingerprinting has gained sufficient acceptance within the mainstream to enable legislators to amend statutes in favor of its use.

---

31. MODEL PENAL CODE § 1.06 cmt. 1 (1985).

32. Bieber, *supra* note 22, at 1089.

33. *Id.* at 1088.

34. DAVID H. KAYE & GEORGE F. SENSABAUGH, JR., REFERENCE GUIDE ON DNA EVIDENCE 506 (2001), *available at* http://www.fjc.gov/public/pdf.nsf/f385048e0431aa3c8525679e0055d35c/e527b2a2ac29ef1c85256a87004590b2/$FILE/sciman09.pdf.

35. *See* Tyler T. Ochoa & Andrew J. Wistrich, *The Puzzling Purposes of Statutes of Limitation*, 28 PAC. L.J. 453, 462 (1997).

36. *See, e.g.*, Veronica Valdivieso, Note, *DNA Warrants: A Panacea for Old, Cold Rape Cases?*, 90 GEO. L.J. 1009, 1042 (2002); Bieber, *supra* note 22, at 1079.

37. Bieber, *supra* note 22, at 1086.

38. *Id.*

39. Interview with Carlos Samour, Deputy Dist. Attorney, Colo. Second Judicial Dist., in Denver, Colo. (Sept. 19, 2005). I note with happiness that then-Deputy District Attorney Samour became Judge Samour, Colorado Eighteenth Judicial District, in December 2006.

40. *See, e.g.*, Corey E. Delaney, Note, *Seeking John Doe: The Provision and Propriety of DNA-Based Warrants in the Wake of Wisconsin v. Dabney*, 33 HOFSTRA L. REV. 1091 (2005); Lisa Schriner Lewis, Note, *The Role Genetic Information Plays in the Criminal Justice System*, 47 ARIZ. L. REV. 519 (2005); Bieber, *supra* note 22, at 1079.

B. The Science of Cold Hits and the "Junk DNA" Question

99.9% of human DNA is identical for all people, so DNA fingerprints must be selected from DNA sequences within the one tenth of one percent that differs between individuals.[41] Thirteen standard identifying loci are used for CODIS samples, representing about one one-millionth of the total human genome.[42] These thirteen loci contain repeated combinations of three to seven base pair units and are called short tandem repeats (STR).[43] Variation in the combinations of base pairs and number of repeats for each of the thirteen CODIS loci enables them to be individually identified.[44] The odds of any two people having identically matching STR at all thirteen CODIS loci approaches one in 575 trillion.[45]

Identification is rarely made on the basis of matching all thirteen loci.[46] Crime scene DNA is seldom that cooperative – DNA suffers degradation due to environmental conditions, contamination, etc. A satisfactory match of DNA fingerprints is declared when the maximum probability of a false match is less than the reciprocal of the U.S. population.[47] It can be stated with "reasonable scientific certainty" that a particular individual is the donor of a given DNA sample when this statistical test is satisfied.[48] Overall, based on the typical number of loci matched and the number of base pairs and repeats at each matched location, the odds of a false positive using the CODIS statistical method approach one in a billion.[49]

The fact that crime scene DNA may be degraded by any number of environmental factors makes it necessary to improve sample quality after collection.[50] The amplification of crime scene DNA samples is accomplished by polymerase chain reaction (PCR), which is described as:

> [a] molecular duplicating process that uses basic cellular chemistry

---

41. HGP, *supra* note 3.

42. David H. Kaye, Commentary, *Two Fallacies About DNA Data Banks For Law Enforcement*, 67 BROOK. L. REV. 179, 188 (2001).

43. HGP, *supra* note 3.

44. *Id.*

45. Sarah L. Bunce, Comment, *United States v. Kincade – Justifying the Seizure of One's Identity*, 6 MINN. J. L. SCI. & TECH. 747, 752 (2005). Note that the global human population is only about 6.5 billion. *See* U.S. Census Bureau, World POPClock Projection, http://www.census.gov/ipc/www/popclockworld.html (last visited Feb. 16, 2007).

46. HGP, *supra* note 3.

47. Bunce, *supra* note 45, at 752. The reciprocal of the U.S. population is approximately 1/301,000,000. *See* U.S. Census Bureau, *supra* note 45.

48. Bunce, *supra* note 45, at 752.

49. HGP, *supra* note 3.

50. *Id.*

> and enzymes to create millions of copies of a desired portion of DNA through repeated cycling of a reaction using heating/cooling. This process enables scientists to obtain DNA information from small or degraded specimens. In forensic science applications, specific sequences of DNA are targeted that are highly variable amongst different individuals [(i.e., the thirteen CODIS loci)].[51]

In other words, crime scene DNA samples that do not include a sufficient quantity of genetic material for accurate laboratory analysis can be duplicated over and over again until the sample size becomes sufficient for reliable analysis. The relatively short length of each STR segment makes it suitable for PCR.[52] After amplification with PCR, the DNA from a sample as small as a few skin cells can yield a reliable match.[53] Even highly degraded samples can often be analyzed – it only takes a few uncompromised cells to initiate successful sample amplification through PCR.[54]

1. "Junk DNA" Explained

Though the entire human genome has been mapped, only 1.4 percent of it is currently believed to contain functioning genes.[55] A gene is defined as a sequence of DNA base pairs that codes for a specific protein.[56] Some of the remaining 98.6% of human DNA may serve regulatory functions, and some non-coding DNA has been identified which indicates predisposition toward certain diseases.[57] However, scientists believe that a significant portion of this non-coding DNA may merely be parasitic DNA inserted by viruses or artifacts of genes made obsolete by human evolution.[58]

Because the thirteen loci used by CODIS do not code for any known protein or indicate any known disease predisposition, they have been described as "junk DNA."[59] This label is somewhat misleading. Some non-coding loci can indicate or predict disease states, and all loci (coding and non-coding alike) can be used for parentage testing.[60] Privacy

---

51. National DNA Databank Glossary, Polymerase Chain Reacton (PCR), http://www.nddb-bndg.org/glossaire_e.htm (last visited Feb. 16, 2007).

52. Bunce, *supra* note 45, at 751.

53. HGP, *supra* note 3.

54. *Id.*

55. Kaye, *supra* note 42, at 188.

56. HGP, *supra* note 3.

57. *See* Ann Gibbons, *Studying Humans – and Their Cousins and Parasites*, 292 SCI. 627, 628 (2001).

58. *Id.*

59. *See* United States v. Kincade, 379 F.3d 813, 837–38 (9th Cir. 2004); Kaye, *supra* note 42, at 188; HGP, *supra* note 3.

60. Kaye, *supra* note 42, at 187 (citing David H. Kaye, *Bioethics, Bench, and Bar: Selected Arguments in Landry v. Attorney General*, 40 JURIMETRICS J. 193 (2000), and R. L.

advocates argue that the STR sequences recorded in CODIS may someday yield information about an individual's medical predispositions, behavior, or heritage despite its non-coding nature, and should therefore be protected.[61] That is, some advocates argue that today's junk DNA may be tomorrow's "window on the soul."[62]

This claim is not yet supported by actual breakthroughs, though we know that non-coding loci can indicate parentage or predict disease states.[63] For example, the condition known as G6PD deficiency causes anemia in humans, and has two variants (of many) that are strongly associated with certain non-coding regions near the G6PD gene.[64] Though the non-coding region near the G6PD gene is not used for CODIS sampling, the fact that non-coding DNA has been shown to contain arguably private genetic information indicates how misleading the label "junk DNA" actually is. This fact suggests to many that the risks of widespread genetic profiling or indefinite retention of biological sample material may outweigh the benefits to the criminal justice system of DNA fingerprinting.[65]

Despite such concerns, there is currently no known potentially compromising genetic information contained among the thirteen CODIS locations other than the fact that they serve as a unique DNA fingerprint that can also confirm familial relationships.[66] The "parentage testing" aspect is sometimes raised by privacy advocates as a further argument against DNA fingerprinting – the fact that DNA can conclusively prove familial relation is held by some to be an intrusion into privacy.[67] However, no rational public policy argument can be offered against accuracy when it becomes the task of the judiciary to sort out parentage. The "window on the soul" argument tends to be the strongest criticism of DNA fingerprinting by privacy advocates, and will be discussed further below.

Alford et al., *Rapid and Efficient Resolution of Parentage by Amplification of Short Tandem Repeats*, 55 AM. J. HUM. GENETICS 190 (1994)).

61. *See* Mark A. Rothstein, *The Impact of Behavioral Genetics on the Law and the Courts*, 83 JUDICATURE 116, 117 (1999) (reporting that scientists are identifying genes that may indicate aggression, sexual orientation, and antisocial behavior).

62. *See id.*

63. *See* Gibbons, *supra* note 57, at 628.

64. *Id.*

65. *See, e.g.*, Press Release, ACLU, ACLU Alarmed At Justice Department Move to Collect DNA, Violates Privacy Rights and Causes Further Delays in Overwhelmed System (Feb. 5, 2007), http://www.aclu.org/privacy/gen/28251prs20070205.html.

66. *See generally* JOHN M. BUTLER, FORENSIC DNA TYPING: BIOLOGY AND TECHNOLOGY BEHIND STR MARKERS (2001); *see also* Kaye, *supra* note 42, at 188; HGP, *supra* note 3.

67. HGP, *supra* note 3.

2. The Possibility of Human Error in DNA Fingerprinting

The possibility of human error in human systems is inherent and should never be ignored. When weighing the value of forensic evidence, the role of human beings in the chain of custody must be considered.[68] As recently as May 2004, a high-profile error in fingerprint analysis by the FBI was acknowledged after an Oregon lawyer was wrongly identified as a participant in the Madrid, Spain train bombings.[69] The possibility of sample contamination at any step in the collection and analysis chain can never be forgotten. Likewise, samples may be mislabeled, mishandled, misplaced, misused or blatantly falsified, as with any crime scene evidence.

Beyond this possibility of human error in collecting, analyzing, and cataloging DNA samples, there remain legitimate questions about the infrastructure that supports DNA fingerprinting. There is well documented evidence of poor management, budget shortages, and corruption within crime labs.[70] In England in 1999, Raymond Easton, a formerly convicted burglar whose DNA fingerprint was on file was wrongly arrested on the strength of a four-loci DNA match between his DNA fingerprint and a sample collected from a crime scene.[71] Easton was charged with burglary based on the four-loci cold hit which, statistically, had only a one in thirty-seven million chance of being a false positive.[72] It was subsequently proven that Easton was two hundred miles away at the time of the crime; additionally, Easton suffered from advanced Parkinson's disease, making it medically impossible that he committed the burglary.[73] Further analysis revealed that two additional DNA loci did not match and Easton was exonerated.[74] Like traditional fingerprint evidence, DNA evidence is only as reliable as the people and processes by which it is collected and analyzed.

---

68. *See, e.g.*, Jennifer L. Mnookin, Op-Ed., *A Blow to the Credibility of Fingerprint Evidence*, BOSTON GLOBE, Feb. 2, 2004, at A14.

69. Susan Schmidt & Blaine Harden, *Lawyer is Cleared of Ties to Bombings: FBI Apologizes for Fingerprint Error*, WASH. POST, May 25, 2004, at A2.

70. *See, e.g.*, Adam Liptak, *The Nation; You Think DNA Evidence is Foolproof? Try Again*, N.Y. TIMES, Mar. 16, 2003, at D5.

71. Jennifer L. Mnookin, *Fingerprint Evidence in an Age of DNA Profiling*, 67 BROOK. L. REV. 13, 49–50 (2001).

72. *Id.*

73. *Id.*

74. *Id.*

III. CRITICISMS: JURY BIAS AND CONSTITUTIONAL PRIVACY

A. Raising and Rebutting the Jury Bias Argument

One criticism of DNA evidence echoes those heard following the introduction of fingerprint evidence at the beginning of the last century. When fingerprint evidence was first allowed by American courts, juries were often offered a "demonstration" of the art by the forensic expert, which often included the expert identifying the jurors themselves by their collected fingerprints.[75] Those demonstrations resembled sideshow mysticism more than *voir dire*, and juries could be blinded to the possibility of human error in this new forensic art by its dazzling power to accurately identify the jury's own members.[76]

DNA evidence is the target of similar criticism of disproportionate influence on juries. As it was with fingerprint evidence, forensic experts very often present DNA evidence in the language of fact, the patois of certainty, rather than in the language of scientific opinion.[77] The perception of DNA's infallibility is so pervasive in the popular culture,[78] it is argued, that the potential for human error during sample collection, preservation, and analysis is overlooked.[79]

While the possibility of human error should never be ignored by legal counsel, particularly in light of continuing fingerprint evidence errors, this possibility is adequately accounted for in our adversarial system. At least one high-profile case argued in recent memory resulted in a not guilty verdict despite "indisputable" DNA evidence.[80] Verdicts like that delivered in the O.J. Simpson murder trial provide at least anecdotal evidence that any prejudicial effect of DNA evidence is balanced by the inherent independence of the jury trial system.[81]

Furthermore, there is evidence that rather than being dazzled by

---

75. *See id.* at 24 (citing People v. Chimovitz, 211 N.W. 650 (Mich. 1927); Stacy v. State, 292 P. 885 (Okla. Crim. App. 1930); Hopkins v. State, 295 S.W. 361 (Ark. 1927)).

76. *Id.* at 26.

77. Mnookin, *supra* note 71, at 28–30.

78. *See* Dr. Kimberlianne Podlas, *"The CSI Effect": Exposing the Media Myth*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 429 (2006); *see also* Kit R. Roane, *The CSI Effect, How TV is Driving Jury Verdicts All Across America*, U.S. NEWS & WORLD REP., Apr. 25, 2005, at 48.

79. *See, e.g.*, Mnookin, *supra* note 68, at A14; Podlas, *supra* note 78, at 437.

80. *See, e.g.*, *CNN Presents: Simple as DNA* (CNN television broadcast Sept. 25, 1995), *available at* http://www.cnn.com/US/OJ/verdict/dna/ (last visited Feb. 16, 2007); *PBS Frontline: Interview with Gerald Uelmen* (PBS television broadcast Oct. 4, 2005) (interviewing former member of the O.J. Simpson defense team and former dean and current Professor of Law at Santa Clara University), *available at* http://www.pbs.org/wgbh/pages/frontline/oj/interviews/uelmen.html.

81. *News and Notes with Ed Gordon: 10 Years After the O.J. Verdict* (NPR Commentary by Clarence Page broadcast, Oct. 3, 2005)

DNA evidence, jury members are now probing sample chains of custody, challenging the credibility of laboratory analysts, and inquiring about the possibility of errors in DNA evidence where trials turn on such evidence.[82] Initially referred to by trial lawyers as the "CSI Effect,"[83] this alleged trend results from juries becoming more sophisticated and critical in their consideration of DNA evidence as forensic science becomes a staple of television news and entertainment.[84] At least one objective study in the legal literature suggests that the "CSI Effect" neither raises the bar for prosecutors attempting to use DNA evidence at trial, nor lowers it through DNA's reputation for infallibility, consistent with the anecdotal evidence discussed above.[85] It appears that the competing practical effects of DNA evidence use at trial cancel one another out. Disposing of the "jury bias" argument leaves us with two serious constitutional concerns.

B. Raising the Fourth Amendment Question

The Fourth Amendment right to be free from unreasonable government intrusion, as explained in *Katz v. United States*, requires a two-pronged analysis: first, a court must determine whether a person has exhibited a subjective expectation of privacy in the matter at issue; if so, the court then asks whether such expectation is ". . . one that society is prepared to recognize as 'reasonable.'"[86] The fact that DNA fingerprinting statutes now include far more felonies than originally contemplated by the Backlog Act,[87] as discussed in more detail below, suggests that our culture is becoming increasingly comfortable with the collection of DNA samples from an ever-widening segment of society.

The Fourth Amendment is implicated only if obtaining a DNA sample from an arrestee constitutes an unreasonable search.[88] DNA evidence found at a crime scene is not the fruit of a search, and is admissible as evidence pursuant to *Katz v. United States*.[89] In *Katz*, the Supreme Court held that what a person chooses to voluntarily expose to

---

82. Telephone Interview with Captain Julie Caruso, U.S. Army Judge Advocate Gen. Corps, in Wash. D.C. (Dec. 27, 2005); *see also* H. Patrick Furman, Clinical Professor of Law, Trial Advocacy Lecture at the University of Colorado Law School (Jan. 11, 2006).

83. H. Patrick Furman, *supra* note 82.

84. Podlas, *supra* note 78, at 461–65.

85. *Id.*

86. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

87. *Compare* source cited *supra* note 16, *with* sources cited *supra* note 20.

88. U.S. CONST. amend. IV ("The right of the people to be secure in their persons . . . against unreasonable searches and seizures, shall not be violated . . . .").

89. *Katz,* 389 U.S. at 347. Note also that biological samples and trace evidence are not testimonial, and therefore do not implicate the Fifth Amendment protection against self-incriminating testimony. *See* Schmerber v. California, 384 U.S. 757 (1966).

the public is not protected by the Fourth Amendment.[90] Biological evidence left by a perpetrator at a crime scene may be seized under the exigency exception to the Fourth Amendment,[91] may be determined to have been voluntarily exposed to the public in accordance with *Katz*, or may be lawfully searched and seized upon the consent of the crime scene property owner. Though rarely necessary under the exigence doctrine, a warrant can generally be obtained if needed to gain access to a crime scene. Regardless of the means by which law enforcement gains access to a crime scene, analysis of crime scene DNA does not implicate the Fourth Amendment with regard to the crime scene DNA donor. However, the involuntary collection of a DNA sample from a federal arrestee does raise the Fourth Amendment question of whether such a sample collection constitutes an unreasonable search of the person or seizure of the DNA.

The federal policy of collecting DNA samples from convicted felons has withstood constitutional challenge.[92] In *Landry v. Attorney General*, a constitutional challenge to the involuntary collection of DNA samples from convicted felons was defeated.[93] The Court held that collection of DNA samples in order to accurately establish the identity of criminals did not implicate the Fourth Amendment.[94] It is now also well settled that, on balance, the government's legitimate interest in an effective and accurate criminal justice system outweighs the diminished privacy rights of convicted felons, making collection of DNA samples from felons a minimal and constitutional intrusion.[95] However, no federal court has yet extended this balance to include arrestees.[96] Though four states have sample-on-arrest statutes, the Supreme Court has not yet considered the question of whether the "diminution of privacy rights" justification extends to arrestees. There is precedent, however, holding that arrestees already have a diminished expectation of privacy.[97] The question remains whether that diminished privacy expectation, when balanced against the government's legitimate interest

90. *Katz*, 389 U.S. at 351.

91. *See, e.g.*, *Schmerber*, 384 U.S. at 757.

92. Landry v. Attorney Gen., 709 N.E.2d 1085, 1092 (Mass. 1999).

93. *Id.*

94. *Id.*

95. *See, e.g.*, United States v. Kincade, 379 F.3d 813, 837–38 (9th Cir. 2004); Rise v. Oregon, 59 F.3d 1556, 1560 (9th Cir. 1995).

96. In *Kincade*, the court was careful to limit its holding to convicted felons, noting that "the DNA act implicates only the rights of convicted felons – not free persons or even mere arrestees." 379 F.3d at 836 n.31.

97. *See* Illinois v. Lafayette, 462 U.S. 640, 643 (1983) (holding that search incident to arrest constitutes a well-defined exception to the Fourth Amendment warrant requirement); United States v. Robinson, 414 U.S. 218 (1973); State v. White, 722 P.2d 118 (Wash Ct. App. 1986) (holding that once arrested, there is a diminished expectation of privacy in the person of the arrestee).

in solving crimes and apprehending criminals, is sufficiently low to allow an unwarranted search upon arrest.

C. Raising the Right to Personal Privacy Question

While the Fourth Amendment privacy question is clearly limited to the "search and seizure" elements of obtaining a DNA sample from a suspect, the personal privacy issue extends to the genetic information that remains unknown or unanalyzed in the biological sample itself. Though DNA fingerprint samples are analyzed for only the thirteen CODIS loci, the sample itself may still contain the entire balance of that individual's genetic code.[98] Because the Act (and its predecessors, such as the Backlog Act) allows the retention of biological samples following analysis, every sampled individual's genetic code potentially remains, unanalyzed, in the hands of the government.

There is a right to privacy that extends beyond the Fourth Amendment protections of privacy vested in persons and possessions. While the constitutional source of such right remains in debate, the Supreme Court has recognized for several years that a right of personal privacy does exist.[99] It is this right that protects individuals from governmental inquiry into matters in which government does not have a legitimate and proper interest.[100] However, the source and extent of this constitutional right to personal privacy remains hotly debated.[101]

The right to personal privacy is most often cited as the basis for the protection from government intrusion into marital intimacy,[102] sexual conduct among consenting adults,[103] the reading of "obscene" materials

98. HGP, *supra* note 3.

99. *See* Lawrence v. Texas, 539 U.S. 558, 595 (2003) (Scalia, J., dissenting) (explaining that the right to personal privacy is grounded in the penumbra of the Bill of Rights) (citing Eisenstadt v. Baird, 405 U.S. 438 (1972)); *see also* Roe v. Wade, 410 U.S. 113, 152 (1973) (holding that the right of privacy is founded in the Fourteenth Amendment's concept of personal liberty). Whether such a right to privacy derives from the Fourteenth Amendment or a constitutional penumbra has little bearing on the question as raised in this note. The personal privacy right protects "two kinds of privacy interests: the individual's interest in avoiding disclosure of personal matters and the interest in being independent when making certain kinds of personal decisions." Eastwood v. Dep't of Corr., 846 F.2d 627, 630–31 (10th Cir. 1988).

100. *See, e.g.*, *Eastwood*, 846 F.2d at 630–31; Whalen v. Roe, 429 U.S. 589, 599–600 (1977) ("The cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.").

101. *See, e.g.*, *Lawrence*, 539 U.S. at 595 (Scalia, J., dissenting); Griswold v. Connecticut, 381 U.S. 479, 508 (1965) (Black, J., dissenting) ("The Court talks about a constitutional 'right of privacy' as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the 'privacy' of individuals. But there is not.").

102. *See, e.g.*, *Eisenstadt*, 405 U.S. at 438; *Griswold*, 381 U.S. at 479.

103. *See, e.g.*, *Lawrence*, 539 U.S. at 558.

in the privacy of one's home,[104] and, of course, reproductive rights.[105] There is not yet any precedent holding that collection of a DNA sample for identification purposes implicates this limited right. While collection of a DNA sample is clearly a Fourth Amendment intrusion, it is not yet clear whether the analysis and storage of a DNA fingerprint from an arrestee will be held to implicate the limited constitutional right to personal privacy. If DNA fingerprints are proven to contain discernable personal information (i.e., if they open a "window on the soul") they would be more deserving of the protection of the limited constitutional right to personal privacy. Moreover, if the retained biological samples collected by law enforcement were to be further analyzed for anything other than CODIS loci, a significant personal privacy issue should be raised.

Privacy advocates argue that even the so-called junk DNA sequences recorded in CODIS may someday yield information about an individual's medical predispositions, behavior, or heritage that is private and should therefore be protected.[106] It is argued that such samples should be collected only from persons whose privacy rights have already been decreased by a criminal conviction, if they are to be collected at all.[107] Even with a "sample on conviction" policy, the argument continues, the biological samples themselves should be destroyed after analysis and codification of the DNA fingerprint. The biological samples, after all, likely contain all of the individual's DNA, not just the thirteen CODIS loci. Therefore, sensitive personal information compromising the individual's genetic privacy rights could be revealed by subsequent re-analysis, either by the FBI or by third parties who obtain the samples.[108]

Despite the above concerns, it appears neither DNA fingerprinting nor CODIS are likely to be abandoned anytime soon. Some objections to DNA evidence can be dismissed as either self-correcting or reflective of the inherent infirmities of human social systems (e.g., jury bias, human error). Current case law holds that the federal "sample on conviction" policy passes constitutional muster on the questions of privacy rights and Fourth Amendment protections. Therefore, two questions remain: (1) whether the "sample on arrest" policy is an unconstitutional intrusion into the genetic privacy of *arrestees* under the constitutional right to personal privacy; and (2) whether involuntary DNA sampling upon arrest

104. *See*, *e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969).

105. *See, e.g.*, Carey v. Population Servs. Int'l, 431 U.S. 678 (1977); *Roe*, 410 U.S. at 113.

106. *See* Rothstein, *supra* note 61, at 117 (pointing out that scientists are identifying genes that may indicate aggression, sexual orientation, and antisocial behavior).

107. *Id.*

108. *See* Kaye, *supra* note 42, at 181 nn.9–11.

constitutes an unreasonable search and seizure under the Fourth Amendment.

IV. THE ARGUMENT IN FAVOR OF THE DNA FINGERPRINT ACT OF 2005

A. The DNA Fingerprint Act of 2005

The Act passed the House of Representatives as stand-alone legislation,[109] was incorporated into the Senate's reauthorization of the Violence Against Women Act,[110] and was signed into law by President Bush on January 5, 2006. The Act authorizes, *inter alia*, collection of DNA samples from persons arrested or detained under federal authority for inclusion in CODIS.[111] At least four states have already passed "sample on arrest" laws,[112] and it is likely that other states will adopt similar legislation now that the Act is federal law.[113] The pertinent parts of the Act appear as Title X of the Violence Against Women Act Reauthorization of 2005:[114]

> The Attorney General may collect DNA samples from individuals who are arrested under the authority of the United States. The Attorney General may collect DNA samples from non-United States persons who are detained under the authority of the United States.
> The Director of the FBI shall promptly expunge from CODIS the DNA analysis of a person against whom charges were dismissed upon receipt of a final court order.
>
> The Director of the FBI shall promptly expunge from CODIS the DNA analysis of a person against whom charges were dismissed, not filed within the applicable time period, or who was acquitted upon

109. DNA Fingerprint Act of 2005, Pub. L. No. 109-162, tit. X, 119 Stat. 2960, 3084; H.R. 2796, 109th Cong. (2005).

110. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1004, 119 Stat. 2960, 3085 (codified as amended at 42 U.S.C. § 14135a).

111. *Id.*

112. *See* CAL. PENAL CODE § 296 (West 2006); LA. REV. STAT. ANN. § 15:609 (2006); NEB. REV. STAT. § 29-4103 (2006); N.J. STAT. ANN. § 53:1-20.20 (West 2007); TEX. GOV'T CODE ANN. § 411.1471 (Vernon 2006); VA. CODE ANN. § 19.2-310.2:1 (2006). Virginia began taking DNA from arrestees in January 2003 and collects about 8,000 samples each year according to Richard Willing*, FBI May Collect Juveniles' DNA*, USA TODAY, Nov. 16, 2003.

113. *See, e.g.*, TIM SCHELLBERG & LISA HURST, APPLIED BIOSYSTEMS, DNA RESOURCE REPORT (2007), *available at* http://www.dnaresource.com/documents/2007_1.pdf. Prior reports posted at this website contain similar synopses of cases involving DNA evidence in the U.S. and abroad.

114. The Act is written as amendments to the DNA Identification Act of 1994 and is best understood within that context. *See* Pub. L. No. 103-322, 108 Stat. 2065 (codified as amended in 42 U.S.C.).

receipt of a final court order.

Simply stated, the Act empowers the Attorney General to collect samples from arrestees and detainees[115] and requires the Director of FBI, as manager of CODIS, to expunge the samples of arrestees that are not subsequently convicted. The statutory expunging requirement mitigates the privacy infringement that arguably results when DNA samples are collected from unconvicted persons, while still allowing ample time for arrestee DNA to be compared to crime scene DNA samples from other unsolved crimes.

B. Arguments in Favor of the Act

The criminal justice system derives many benefits from the use of DNA fingerprints. DNA fingerprinting provides a more positive form of identification than the collection of conventional fingerprints, mug shot photography, recording a physical description, or other conventional methods because there is no known method of altering or temporarily eradicating one's genetic code.[116] It has been argued that DNA data does, in fact, increase "the accuracy of the criminal justice system,"[117] and this is persuasive. If the accurate identification of persons in the custody of the federal government was the primary goal of CODIS, then taking DNA samples upon arrest for a federal offense would probably satisfy a "rational basis" test. But though it is unquestionably a valuable characteristic of CODIS, "accuracy" is only a secondary benefit of DNA fingerprinting.[118] The primary legislative intent behind CODIS is the generation of investigative leads.[119] Therefore, the Fourth Amendment question remains: does collection of a DNA sample upon arrest constitute an unreasonable search? If not, then the Act is likely constitutional.

1. Response to Fourth Amendment Challenges

Under a *Katz* analysis, collecting DNA fingerprints from federal arrestees violates the Fourth Amendment if it satisfies both prongs of a two-pronged test.[120] First, the arrestee must have a subjective

115. This language may be directed toward PATRIOT Act detainees and is outside the scope of this casenote, but it certainly deserves further consideration and analysis.

116. Of course, the fact that DNA cannot be altered or eradicated precludes a *Schmerber* justification for sampling upon arrest. Schmerber v. California, 384 U.S. 757 (1966). In *Schmerber*, the Court held that a search incident to a valid arrest can include blood testing (in this case, to determine blood alcohol content) where fruits or evidence might be destroyed or concealed if not recovered (in this case, by normal human metabolism). *Id.*

117. United States v. Reynard, 220 F. Supp. 2d 1142, 1167 (S.D. Cal. 2002).

118. Kaye, *supra* note 42, at 203.

119. *Id.*

120. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

expectation that his DNA fingerprint is private.[121] Assuming, *arguendo*, that the first federal arrestee subjected to the Act had such an expectation, the second prong of *Katz* asks whether such a privacy expectation is one that society is prepared to recognize as reasonable.[122] The Fourth Amendment analysis therefore turns on whether society recognizes as reasonable an arrestee's expectation of privacy for his DNA fingerprint. Given the current fascination with DNA use in criminal justice,[123] and the success of recent legislation which expanded the use of DNA to fight crime,[124] there is a legitimate argument to be made that society does not hold reasonable an arrestee's expectation that his DNA fingerprint is private. Particularly in light of other existing safeguards (e.g., probable cause still required), and the narrow tailoring of the statute (e.g., mandatory expunging of arrestee DNA fingerprints from CODIS upon acquittal), a sample on arrest policy may well satisfy the *Katz* test as a reasonable intrusion into Fourth Amendment privacy.

Both well-settled case law and recent precedents will limit the government intrusions into Fourth Amendment rights that may arise under the Act. In *Davis v. Mississippi*, the Supreme Court held in 1969 that fingerprints obtained during an illegal arrest and detention were inadmissible as evidence.[125] The Court reaffirmed this position in 1985 when it decided *Hayes v. Florida*.[126] Though fingerprinting was recognized as less intrusive into an individual's private life and thoughts than an interrogation, and likewise less harassing than repeated contacts by police, the Court still required probable cause under the Fourth Amendment before a suspect could be arrested in order to procure his fingerprints.[127] The Court recognized the probative value of fingerprinting, calling it "inherently more reliable and effective" than eyewitness identifications or confessions, but maintained that the relevance and trustworthiness of illegally obtained evidence could not outweigh the constitutional prohibitions against such use.[128] A suspect may not be "apprehended, detained, and forced to accompany police to another location to be fingerprinted without a warrant or probable

121. *Id.*
122. *Id.*
123. *See supra* note 78.
124. *See supra* notes 16–19.
125. 394 U.S. 721 (1969).
126. 470 U.S. 811, 813 (1985) (where there was no probable cause to arrest suspect, suspect did not consent to journey to police station, and there was no prior judicial authorization for detaining him, investigative detention at police station for fingerprinting purposes violated petitioner's rights under Fourth Amendment; hence, fingerprints taken were the "inadmissible fruits of an illegal detention").
127. *Davis*, 394 U.S. at 724.
128. *Id.*

cause."[129] These precedents should also apply to DNA fingerprinting, thereby preventing invalid arrest as a pretext for the collection of DNA samples.

The United States Court of Appeals for the Ninth Circuit recently reviewed a matter of first impression regarding warrantless searches in *United States v. Scott*.[130] The reasoning of that case further illustrates the commitment of the judiciary to Fourth Amendment protections that will still apply under the Act. The Ninth Circuit held that mandatory drug testing cannot be imposed as a condition of pretrial release because it would violate the Fourth Amendment requirement for probable cause.[131] While the government may detain an arrestee or require bond to ensure his presence at trial, the government may not extract waivers of constitutional rights in exchange for benefits such as pre-trial release, even when those benefits are fully discretionary.[132]

An individual's consent to a warrantless search is only valid if the search itself is reasonable, regardless of whether the individual consented to such a search as a condition of pretrial release.[133] Under this precedent, a person could not constitutionally consent to DNA fingerprinting as a condition of custodial release; the government would have to show probable cause for arrest prior to any DNA fingerprinting. Where *Davis* and *Hayes* should preclude wrongful arrest as a pretext to obtain DNA fingerprints, *Scott* should preclude coercive DNA fingerprinting as a condition of release from custody (though, if the custodial arrest was valid, the Act requires DNA fingerprinting without further consent).

These precedents suggest that Fourth Amendment protections remain adequate under the Act. The fact that an arrestee's DNA fingerprint may connect them to other crimes is of no consequence to the Fourth Amendment analysis; it is no different than an arrestee's traditional fingerprints connecting him to another crime. The clear legislative intent behind DNA fingerprinting is to generate investigative leads and improve the accuracy of the criminal justice system, which is analogous to traditional fingerprinting, and therefore, DNA fingerprinting should receive the same Fourth Amendment protections as traditional fingerprinting.[134] Though arrestees are presumed innocent, a

129. *Hayes*, 470 U.S. at 818–19 (Brennan, J., concurring).

130. 424 F.3d 888 (9th Cir. 2005), *amended by*, 450 F.3d 863 (9th Cir. 2005).

131. *Id.* at 893.

132. *Id.* at 890–91.

133. *Id.* at 893.

134. *See* Napolitano v. United States, 340 F.2d 313, 314 (1st Cir. 1965) ("Taking of fingerprints in such circumstances is universally standard procedure, and no violation of constitutional rights."); Smith v. United States, 324 F.2d 879, 882 (D.C. Cir. 1963) (holding that "a person in lawful custody may be required to submit to . . . fingerprinting . . . as part of

valid arrest necessarily satisfies the probable cause required to detain the arrestee to answer for a crime.[135] If an arrest is valid, the subsequent search of the individual incident to arrest is also valid.[136] A person validly arrested has diminished expectations of privacy as a result of his arrest and detention.[137] Under a *Katz* analysis, if society does not recognize an expectation of privacy in an arrestee's DNA, a "search" of an arrestee's DNA would not be unreasonable.

Even if society does recognize a reasonable expectation of privacy in an arrestee's DNA fingerprint under *Katz*, a Fourth Amendment balancing test that weighs the government's legitimate and narrowly tailored interest in obtaining DNA fingerprints against the arrestee's diminished privacy interest should favor the government. Unless, and until, DNA fingerprinting is proven to reveal more about an arrestee than a unique and unchanging identification code, the value of DNA fingerprinting far outweighs the privacy intrusion on the affected individuals.[138]

Some observers have compared DNA analysis by law enforcement, with its potential for revealing a vast quantity of personal genetic information, to the widespread abuses that followed the introduction of wiretapping as an investigatory tool.[139] In *Olmstead v. United States*, the Supreme Court held that wiretapping did not infringe on the Fourth Amendment unless a physical trespass was implicated.[140] Subsequent history is replete with abuses by law enforcement, arguably culminating with the current Administration's domestic spying scandal,[141] though

---

the routine identification process"). Interestingly, it may soon be possible to obtain DNA samples from the skin oils that form crime scene fingerprints. Like the saliva left on a cigarette butt found at a crime scene, DNA samples obtained from skin oils left on surfaces would not implicate the Fourth Amendment under *Katz* because such oils would arguably have been exposed to public view, just like the other crime scene evidence. If no bodily intrusion was necessary to collect a DNA sample (i.e., if a suspect's skin oils were deposited on a paper coffee cup which the suspect then discarded), would its analysis and inclusion in CODIS as a DNA fingerprint be treated under Katz as if it were exposed to the public? *See* Rothstein & Carnahan, *supra* note 6, at 144–45.

135. Cupp v. Murphy, 412 U.S. 291, 301 (1973) (Douglas, J., dissenting in part) (defining arrest as "the taking of a person into custody so that he may be held to answer for a crime.") (citing OR. REV. STAT. § 133.210 (1972)).

136. Illinois v. Lafayette, 462 U.S. 640, 643 (1983) (affirming that a search incident to arrest constitutes a well-defined exception to the Fourth Amendment warrant requirement).

137. State v. White, 722 P.2d 118 (Wash. Ct. App. 1986).

138. Judge Morris B. Hoffman of the Colorado Second Judicial District raises the interesting question of whether the Fifth Amendment might one day be implicated by DNA. If DNA fingerprints are found one day to reveal evidence of a genetic propensity toward violence or sexual deviancy, or any "antisocial" trait, would that information become "testimonial" and therefore subject to Fifth Amendment analysis? This question is not ripe at present, given our limited understanding of the human genome, but is certainly worthy of further consideration.

139. *See generally* Kaye, *supra* note 42, at 193.

140. 277 U.S. 438, 466 (1928).

141. *See, e.g.*, Eric Lichtblau & James Risen, *Domestic Surveillance: The Program; Spy*

Olmstead has since been overruled and wiretapping is now much more tightly regulated.[142]

But DNA databases do not interfere with personal communication or track a person's movements like intercepted communications. Justice Brandeis' later-validated concerns with widespread wiretapping, expressed in his *Olmstead* dissent,[143] are not implicated by the Act because, unlike *Olmstead*-era wiretapping, there are now sufficient Fourth Amendment protections recognized by the judiciary to prevent the abuses that followed *Olmstead*.[144] Fourth Amendment fears must be balanced against the potential benefit of identifying offenders more quickly, potentially before their criminal conduct recurs or escalates, based on trace evidence that matches a CODIS sample.

2. Response to "Penumbra" Personal Privacy Challenges

As already discussed, the legislative intent behind the creation of CODIS was primarily to generate leads in criminal investigations. The expanding use of DNA evidence to generate suspects, rather than solely to support the prosecution of individuals already charged with crimes, fuels fears of diminished personal privacy resulting from DNA sample collection and storage.[145] The Act proposes to greatly expand the number of persons affected by DNA fingerprinting, whose entire genetic code would remain potentially intact, though unanalyzed, in the stored biological sample. The potential for abuse of such information cannot be ignored. Accordingly, this analysis must consider and resolve these personal privacy issues.

There is evidence that privacy concerns are overstated. Biological samples have long been used by forensic scientists to identify individuals.[146] For example, blood proteins and serum groups have long been accepted as forensic evidence even though such samples can contain the entire genetic code and other potentially sensitive biological

---

Agency Mined Vast Data Trove, Officials Report, N.Y. TIMES, Dec. 24, 2005, at A1; *see generally* BOB WOODWARD & CARL BERNSTEIN, ALL THE PRESIDENT'S MEN (1974) (describing illegal wiretapping by Presidential order at the Watergate Hotel).

142. *See Katz*, 389 U.S. at 347; Berger v. New York, 388 U.S. 41 (1967).

143. *Olmstead*, 277 U.S. at 474–75 ("[I]n the application of a Constitution, our contemplation cannot be only of what has been, but of what may be . . . [i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . .").

144. *See* Kaye, *supra* note 42, at 193.

145. *See* Richard Willing, *Bill Would Expand U.S. DNA Database*, USA TODAY, Oct. 2, 2005, *available at* http://www.usatoday.com/news/washington/2005-10-02-dna-database-bill_x.htm.

146. Kaye, *supra* note 42, at 187.

information.[147] In the words of Professor David H. Kaye, a frequent and respected contributor to this debate, "[i]t serves no clear purpose to bar access to [DNA] loci that are not indicative of features of some social concern."[148]

Likewise, there are no known instances of CODIS data disclosure to any inappropriate third party.[149] Though no electronic database, federal or otherwise, can ever be completely secure in the Internet Age, it is unreasonable to declare CODIS data to be a significant risk to individual liberty and privacy in the absence of a documented wrongful disclosure or even a credible threat. Consider also that the U.S. Department of Defense has maintained a database of DNA fingerprints for all service members, for the purpose of identifying remains, since the late 1980's[150] with no known instances of inappropriate disclosure. In short, there is not yet compelling evidence that individual privacy will be compromised by DNA fingerprinting of arrestees. Note that when forensic fingerprinting first gained popularity, it was proposed that the secrets of an individual's heritage and personality could be deciphered from his fingerprints.[151] These claims were proven unfounded, and fingerprinting was ultimately accepted as the benign identification tool that we recognize today.[152] Additionally, the fact that DNA is color-blind should weigh in favor of the Act.[153]

The other source of concern is the biological samples themselves. These have the potential to reveal far more information than the CODIS fingerprint because the entire genome may exist within the sample.[154] The FBI opposes the destruction of stored biological samples, though these are arguably the most potentially sensitive element of the DNA

147. *Id.*

148. *Id.*

149. Searches of Westlaw, Lexis-Nexis and other resources revealed no reports of CODIS data compromise as of February 2007. As author M. Dawn Herkenham explains, "[t]he unauthorized disclosure of DNA information is subject to a criminal fine not to exceed $250,000, or imprisonment for a period not to exceed one year. Obtaining DNA samples or DNA information, without authorization, is punishable by a maximum fine of $250,000 or imprisonment for not more than one year or both fine and imprisonment." M. Dawn Herkenham, *Retention of Offender DNA Samples Necessary to Ensure and Monitor Quality of Forensic DNA Efforts*, 34 J.L. MED. & ETHICS 380, 382 (2006) (citing 42 U.S.C. §§ 14133(c), 14135e(c) (2004)).

150. U.S. Dep't of Def. Instruction No. 5154.30, Armed Forces Institute of Pathology Operations (Mar. 18, 2003), *available at* http://www.dtic.mil/whs/directives/corres/pdf/515430p.pdf.

151. *See* Mnookin, *supra* note 71, at 33–34.

152. *Id.*

153. Kaye, *supra* note 42, at 196. For example, a New Orleans murder suspect was believed to be African American, based on witness statements, until crime scene DNA showed he was Asian.

154. HGP, *supra* note 3.

fingerprinting process.[155] Reasons for the FBI's opposition include:

(1) to maintain uniformity among the states, because virtually all states require sample retention; (2) to avoid the prohibitive cost of re-typing convicted offenders once they have been released from prison, should it be necessary; (3) to assure data base consistency among the states in light of technological advances; (4) to allow re-checking a hit against the sample to assure a sample has not been mistyped, thus avoiding the release of a person's name to law enforcement personnel by mistake; and (5) that it is safe to retain samples because no abuse of stored samples has been reported in over ten years of databasing.[156]

Ironically, the assertion that CODIS, like any electronic database, should not be considered completely secure against electronic penetration may be the strongest argument in favor of biological sample retention. In the event that CODIS were compromised, the biological samples would remain as low-tech backups. If retained DNA samples are abused, through government analysis beyond the thirteen CODIS loci or release to third parties, the simplest and most expedient solution is to destroy the biological samples once the CODIS fingerprint is determined.

Privacy advocates often cite the increasing body of knowledge regarding genetic predispositions, such as an alcohol addiction predisposition, as a basis for genetic privacy fears.[157] To suggest that such genetic predispositions would prejudicially affect an individual's treatment by the criminal justice system ignores our system of law. Our legal system judges people on the basis of their conduct, not their genes.[158] Our criminal justice system is predicated on a belief in free will, not genetic predisposition.[159] The Federal Rules of Evidence already bar the use of "conformity" evidence with regard to character[160]; evidence of "genetic conformity" should similarly be barred. Additionally, many states already have "genetic property rights" statutes,[161] and equivalent federal law is being considered to prevent against wrongful possession or use of genetic information.[162]

---

155. Dr. Tom Callaghan, Program Manager, FBI, Remarks to the National Commission on the Future of DNA Evidence (Sept. 26, 1999), *available at* http://www.ojp.usdoj.gov/nij/topics/forensics/events/dnamtgtrans7/trans-c.html.

156. *Id.*

157. *See, e.g.*, Lee M. Silver, *The Meaning of Genes and "Genetic Rights"*, 40 JURIMETRICS J. 9, 17–18 (1999).

158. *See, e.g.*, Lewis, *supra* note 40, at 544.

159. *Id.*

160. FED. R. EVID. 404 (a)-(b) (prohibiting admission of character evidence to show conduct in conformity therewith).

161. *See, e.g.*, COLO. REV. STAT. § 10-3-1104.7 (2006) ("Genetic information is the unique property of the individual to whom the information pertains."); S.C. CODE ANN. § 38-93-30 (1998); Kaye, *supra* note 42, at 181 n.5.

162. *See, e.g.*, H.R. 1227, 109th Cong. (2005); S. 306, 109th Cong. (as passed by Senate, Feb. 17, 2005).

Currently, there is no compelling evidence that DNA fingerprinting will compromise personal privacy if its collection were to include arrestees; however, evidence that adding arrestees to CODIS will generate increased cold hits is undeniable. The FBI claims a cold-hit rate of only twenty-two percent using CODIS.[163] United Kingdom law enforcement officials, who follow a "sample on arrest" policy, claim a cold-hit rate of almost forty percent.[164] Most cold matches in England and New Zealand, where "sample on arrest" policies have been in place for years, come between crime scene DNA and the DNA fingerprints of burglary suspects and convicts.[165] Recidivism rates for felons are high and repeat offenders are common; more importantly, many persons ultimately convicted of violent felonies were previously arrested for lesser crimes, but released.[166] By expanding the CODIS population to include arrestees, the chances of a cold hit will increase based on the established patterns of repeat criminal conduct.

Finally, and perhaps most importantly, the Act requires the expunging of DNA fingerprints from CODIS for those persons who are exonerated, against whom charges are dropped, or against whom charges are not filed within the required time period.[167] In this way, the impact of the Act on the legitimate privacy concerns of innocent parties is mitigated.[168]

On balance, the benefits of the DNA Fingerprinting Act of 2005

---

163. *See* Federal Bureau of Investigation – Combined DNA Index System (CODIS) Home Page, http://www.fbi.gov/hq/lab/codis/index1.htm (last visited Apr. 2006) (noting that 27,700 cold hits had been generated from 124,285 crime scene DNA samples as of Nov. 2005).

164. Press Release, Forensic Sci. Serv., Crime Reduction Model (July 14, 1999) (on file with author).

165. *See*, *e.g.*, S.A. Harbison et al., *The New Zealand DNA Databank: Its Development and Significance as a Crime Solving Tool*, 41 SCI. & JUST. 33, 36 (2001) (reporting that 77% of reported database matches in New Zealand originated from burglaries); David Werrett, The Strategic Use of DNA Profiling, Address to the 18th International Congress of Forensic Haemogenetics (Aug. 19, 1999).

166. *See* LAWRENCE A. GREENFELD, U.S. DEP'T OF JUST., SEX OFFENSES AND OFFENDERS: AN ANALYSIS OF DATA ON RAPE AND SEXUAL ASSAULT 26–27 (1997) (rates of re-arrest and re-conviction for rapists were 52% and 36%, respectively; for all violent offenders, rates were 60% and 42%, respectively).

167. Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 1002, 119 Stat. 2960, 3084-85 (codified at 42 U.S.C. § 14132).

168. *See also UK Police Chief Calls for a National DNA Database*, 393 NATURE 106 (1998); *but see* David H. Kaye & Michael E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413 (2003); Akhil Reed Amar, *A Safe Intrusion*, AM. LAW., June 2001, at 69 (advocating establishment of DNA data bank for all citizens, but requiring some of the precautions considered in this note, such as destruction of samples after analysis and analyzing only non-coding regions of the genome). The "expunging" provision of the Act is a significant factor in the balance favoring adoption of the Act; the absence of such a provision tilts the balance away from universal DNA sampling.

outweigh the risks. The balance between the competing interests of solving crimes and assuring genetic privacy must tilt toward optimizing the identification of criminal suspects, unless the privacy intrusions predicted by some to arise from DNA collection become manifest. Furthermore, Fourth Amendment concerns prove groundless once it is shown that DNA sample collection and analysis does not violate a detainee's diminished expectation of privacy. If privacy concerns are satisfied, then DNA fingerprinting can reasonably be treated as a "high-tech" alternative to traditional fingerprinting and employed in a constitutionally similar manner. Absent legitimate privacy concerns predicated on the compromise of CODIS data or the wrongful release of biological samples (which could be destroyed if necessary to prevent such a potential release), the constitutional protections against obtaining traditional fingerprints as the fruit of an unreasonable search should be adequate to protect against the abuse of DNA fingerprinting.

V. CONCLUSION

The DNA Fingerprint Act of 2005 adds the DNA fingerprints of persons arrested for federal offenses to CODIS, greatly expanding the CODIS sample population and thereby increasing the probability of obtaining cold hits. This approach is practiced in the United Kingdom and other western nations, which report cold-hit rates between crime scene DNA and individual DNA of almost double the rate such matches are generated in the United States. There is no reason not to expect similar success in suspect generation through crime scene DNA matching in this country. The one practical objection to the increased use of DNA in criminal justice that is not true of all forensic evidence is the claim that the persuasive power of DNA evidence outweighs its probative value. However, there is sufficient anecdotal evidence to illustrate that juries treat DNA evidence as skeptically as any other forensic evidence. In fact, emerging trends may indicate that the popular culture's fascination with DNA evidence may actually have raised the bar on its acceptance by juries.

The two principled objections to adopting a "sample on arrest" policy turn on privacy. Though a Fourth Amendment argument is often raised when the issue is debated, DNA fingerprinting is not fundamentally different from traditional fingerprinting once the privacy questions are resolved. The Fourth Amendment protections against illegal search and seizure that prohibit taking an individual's fingerprints without probable cause should extend to that individual's DNA fingerprint. Therefore, the Fourth Amendment issue should be well settled under existing case law by analogizing DNA fingerprinting to traditional fingerprinting.

The real issue is whether collection and retention of a biological sample, and the codification of a DNA fingerprint from that sample, creates an unbearable risk to individual liberty and personal privacy for persons presumed innocent. Persons convicted of felonies have diminished privacy and liberty rights, so the minimally-intrusive collection of their DNA fingerprints does not raise a constitutional question. But arrestees remain innocent until proven guilty, so the collection and analysis of DNA from arrestees raises privacy questions if their DNA fingerprints contain information worthy of constitutional protection.

Our society does not consider information that describes height, eye color, hair color, etc., to be worthy of privacy protection. Likewise, identification by fingerprints has long been accepted as minimally intrusive and unworthy of privacy protection (though, of course, protected by the Fourth Amendment). If we are to treat DNA fingerprints differently, that treatment must be based on a reasonable belief founded on actual events that the information contained in our DNA fingerprints is worthy of privacy protection. Though new discoveries about the content of our genetic code are frequently announced, science has not yet shown that the thirteen CODIS loci contain any information worthy of constitutional protection. Additionally, the CODIS database itself (and private genetic databases, for that matter) have, thus far, not been the target of significant acts of fraud or data compromise.

Likewise, the biological samples themselves, which the FBI retains after analysis, create no more risk to individual liberty and privacy than a blood sample provided to a physician – while both likely contain the entire genetic code of the donor, both are safeguarded against compromise. In fact, blood protein matching and serum typing has played a role in both civil and criminal jurisprudence for generations, so the use of biological sampling is hardly unprecedented. Add in the fact that DNA fingerprinting is "color-blind," has exonerated a significant number of wrongly-convicted individuals, does not degrade over time like most evidence, supports the issuance of "John Doe" warrants to ensure that justice can be done, and provides a unique and precise means of accurate identification when correctly interpreted, and the balance clearly favors the constitutionality of the Act.