

# JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

University of Colorado Law School  
320-L Wolf Law Building, 401 UCB, Boulder, CO 80309-0401  
+1.303.735.1032 • [info@jthtl.org](mailto:info@jthtl.org) • <http://jthtl.org>

POSTMASTER: Please send address changes to the address above.

The Journal on Telecommunications and High Technology Law is an association of students sponsored by University of Colorado Law School and the Silicon Flatirons Center for Law, Technology, and Entrepreneurship.

## *Subscriptions*

Issues are published semiannually. Domestic volume subscriptions are available for \$45.00. City of Boulder subscribers add \$3.74 sales tax. Boulder County subscribers outside the City of Boulder add \$2.21 sales tax. Metro Denver subscribers outside of Boulder County add \$1.85 sales tax. Colorado subscribers outside of Metro Denver 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 [subscriptions@jthtl.org](mailto:subscriptions@jthtl.org) or by mail to the address above. Back issues in sets, volumes, or single issues may be obtained from:

William S. Hein & Co., Inc.  
1285 Main Street, Buffalo, NY 14209  
p: 1.716.882.2600 • <http://www.wshein.com>  
<http://heinonline.org> (for back issues in electronic format)

## *Manuscripts*

JTHTL invites the submission of unsolicited manuscripts exclusively via electronic delivery. Submissions may be e-mailed directly to [submissions@jthtl.org](mailto:submissions@jthtl.org) or submitted via ExpressO (<http://law.bepress.com/expresso>) or LexOpus (<http://lexopus.wlu.edu/>). Please include a curriculum vitae and cover letter. JTHTL uses THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (19th ed. 2010) and THE CHICAGO MANUAL OF STYLE (14th ed. 2003).

Cite as: 9 J. ON TELECOMM. & HIGH TECH. L. \_\_ (2011).

©2011, Journal on Telecommunications and High Technology Law.



# JOURNAL ON TELECOMMUNICATIONS & HIGH TECHNOLOGY LAW

Volume 9

Spring 2011

## BOARD OF EDITORS

*Editor-in-Chief*  
ERIC P. SCHMIDT

*Managing Editor*  
ALISON JENSEN

*Executive Editor*  
CATHERINE HOLTGREWE

*Lead Production Editor*  
THERESE KERFOOT

*Associate Production Editor*  
JAKE ADKINS

*Resource Editor*  
CHRISTIAN ALEXANDER

*Executive Articles Editor*  
JENNIFER McDONALD

*Executive Student Note Editor*  
KIMBERLY WEST

*Articles Editors*  
SHIRIN CHAHAL  
ANGELA MORRISON  
MEREDITH SIMMONS

*Student Note Editors*  
DESTA ASFAW  
KAZUYO MORITA  
REBECCA SISKA-SALKIN  
ANGELA WADE

## EDITORIAL STAFF

*Associate Editors*  
VLAD ETINGER  
TAWNYA FERBIK  
CHRISTINE RINKE

*Symposium Editor*  
MADELAINE MAIOR

*Associate Symposium Editor*  
JANNA FISCHER

## MEMBERS

KENDRIA ALT  
KRISTIN BAILEY  
JOHN BESKI  
CAROLYN BLACK  
SARAH BOULDEN  
DOUG BRAKE  
ZACHARY BROWN  
CANDYCE CHOI

DAVID CLINE  
ANGELA COLEMAN  
CHRISTOPHER COOK  
MAINAK D'ATTARAY  
WILLIAM FISCHER  
LISA FISCHER  
JEFFREY GRAVES  
DAMION LEE NATALI

JESSICA MORGAN  
BRENT OWEN  
SARA RADKE  
CHRISTOPHER STANTON  
MICHAEL STUZYSKI  
NICHOLAS WEST  
MARK WIRANOWSKI  
JOHN ZWICK

FACULTY ADVISORS  
PAUL OHM  
HARRY SURDEN

OFFICE MANAGER  
MARTHA S. UTCHENIK



# UNIVERSITY OF COLORADO LAW SCHOOL

## Faculty, 2010-2011

### *Deans*

- DAVID H. GETCHES, *Dean and Raphael J. Moses Professor of Natural Resources Law*. A.B., Occidental College; J.D., University of Southern California.
- DAYNA BOWEN MATTHEW, *Associate Dean for Academic Affairs and Professor of Law*. A.B., Harvard-Radcliffe College; J.D., University of Virginia.
- SARAH A. KRAKOFF, *Associate Dean for Research and Professor of Law*. B.A., Yale University; LL.B., University of California, Berkeley.
- WHITING LEARY, *Senior Assistant Dean for Students*. B.A., Williams College; J.D., University of Colorado.
- SUSANI HARRIS, *Assistant Dean for Career Development*. B.A., University of Colorado; M.A., University of Arizona; J.D., University of Denver College of Law.
- KRISTINE M. JACKSON, *Assistant Dean for Admissions and Financial Aid*. B.S., University of North Carolina; J.D., George Mason University.

### *Emeritus Faculty*

- NORMAN F. AARONSON, *Clinical Professor Emeritus, Legal Aid and Defender Program*. A.B., Brandeis University; J.D., Boston University.
- CLIFFORD J. CALHOUN, *Professor Emeritus*. A.B., LL.B., Harvard University.
- HOMER H. CLARK, JR., *Professor Emeritus*. A.B., LL.D., Amherst College; LL.B., LL.M., Harvard University.
- JAMES N. CORBRIDGE, JR., *Professor Emeritus*. A.B., Brown University; LL.B., Yale University.
- TED J. FIFLIS, *Professor Emeritus*. B.S., Northwestern University; LL.B., Harvard University.
- H. PATRICK FURMAN, *Clinical Professor Emeritus, Legal Aid and Defender Program, and Director of Clinical Programs*. B.A., J.D., University of Colorado.
- DAVID S. HILL, *Professor Emeritus*. B.S., J.D., University of Nebraska.
- 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.
- 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 E. RENTFRO, *Professor Emeritus*. B.A., University of Colorado; Th.M., LL.B., University of Denver.
- PETER N. SIMON, *Professor Emeritus*. B.S., M.D., University of Wisconsin; J.D., University of California, Berkeley.

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.

*Tenured and Tenure-Track Faculty*

BARBARA A. BINTLIFF, *Nicholas Rosenbaum Professor of Law and Law Library Director*. B.A., Central Washington State College; J.D., M.L.L., University of Washington.  
WILLIAM BOYD, *Associate Professor of Law*. Ph.D., University of California, Berkeley; J.D., Stanford University.  
HAROLD H. BRUFF, *Charles Inglis Thomson Professor of Law*. B.A., Williams College; J.D., Harvard University.  
ALEXIA BRUNET MARKS, *Associate Professor of Law*. B.A., Colgate University; M.S., Purdue University; Ph.D., Purdue University; J.D., Northwestern University.  
EMILY M. CALHOUN, *Professor of Law*. B.A., M.A., Texas Tech University; J.D., University of Texas.  
PAUL F. CAMPOS, *Professor of Law*. A.B., M.A., J.D., University of Michigan.  
DEBORAH J. CANTRELL, *Director of Clinical Programs and Associate Professor of Law*. B.A., Smith College; M.A., University of California, Los Angeles; J.D., University of Southern California.  
KRISTEN CARPENTER, *Associate Professor of Law*. B.A., Dartmouth College; J.D., 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.  
NESTOR DAVIDSON, *Associate Professor of Law*. A.B., Harvard University; J.D., Columbia University.  
JUSTIN DESAUTELS-STEIN, *Associate Professor of Law*. B.A., University of North Carolina, Asheville; J.D., University of North Carolina, Chapel Hill; LL.M., Harvard University.  
MIRANDA P. 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., J.D., University of Chicago.  
WAYNE M. GAZUR, *Professor of Law*. B.S., University of Wyoming; J.D., University of Colorado; LL.M., University of Denver.  
MARISA AYA GRUBER, *Professor of Law*. B.A., University of California at Berkeley; J.D., Harvard Law School  
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.  
CLARE HUNTINGTON, *Associate Professor of Law*. B.A., Oberlin College; J.D., Columbia University.  
MARK J. LOEWENSTEIN, *Nicholas A. Rosenbaum Professor of Law*. A.B., J.D., University of Illinois.  
SCOTT A. MOSS, *Associate Professor of Law*. B.A., M.A., Stanford University; J.D., Harvard 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.

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

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

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

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., J.D., Stanford University.

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

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

ANDREW SCHWARTZ, *Associate Professor of Law*. Sc.B., Brown University; J.D., Columbia University.

ANNA SPAIN, *Associate Professor of Law*. B.A., Denison University; J.D., Harvard University.

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

HARRY SURDEN, *Associate Professor of Law*. B.A., Cornell University; J.D., Stanford University.

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

PHILIP J. WEISER, 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 Emeritus, Legal Aid and Defender Program*. A.B., Brandeis University; J.D., Boston University.

J. BRAD BERNTHAL, *Associate Clinical Professor of Law*. B.A., University of Kansas; J.D., University of Colorado.

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

VIOLETA CHAPIN, *Associate Clinical Professor of Law*. B.A., Columbia College; J.D., New York University.

- MARGARET ANN ENGLAND, *Associate Clinical Professor, Legal Aid and Defender Program*. B.A., University of Michigan; J.D., University of Denver.
- H. PATRICK FURMAN, *Clinical Professor Emeritus, Legal Aid and Defender Program, and Director of Clinical Programs*. B.A., J.D., University of Colorado.
- COLENE ROBINSON, *Associate Clinical Professor, Juvenile and Family Law*. B.A., Valparaiso University; J.D., Loyola University School of Law, Chicago.
- JILL E. TOMPKINS, *Clinical Professor of Law and Director of American Indian Law Clinic*. B.A., The King's College; J.D., University of Maine.

*Legal Writing and Appellate Advocacy Faculty*

- AL CANNER, *Legal Writing Professor*. B.A., Brandeis University; J.D., University of Colorado.
- AMY BAUER, *Legal Writing Professor*. B.A., Duke University; J.D., William & Mary School of Law.
- DEREK H. KIERNAN-JOHNSON, *Legal Writing Professor*. A.B. Princeton University; J.D., University of Michigan.
- NATALIE MACK, *Legal Writing Professor*. B.S., University of South Carolina; J.D., University of Colorado.
- GABRIELLE M. STAFFORD, *Legal Writing Professor*. B.A., University of Pennsylvania; J.D., Boston University.
- TODD M. STAFFORD, *Legal Writing Professor*. B.A., Southern Methodist University; J.D., Duke University.

*Law Library Faculty*

- BARBARA A. BINTLIFF, *Nicholas Rosenbaum Professor of Law and Law Library Director*. B.A., Central Washington State College; J.D., M.L.L., University of Washington.
- ALICIA BRILLON, *Reference Librarian*. B.A., M.L.I.S., University of Washington; J.D., Seattle University.
- GEORGIA K. BRISCOE, *Associate Director and Head of Technical Services*. B.S., Washington State University; M.A., University of San Diego; M.L.S., University of Michigan.
- YUMIN JIANG, *Technical Services Librarian*. M.S., University of Illinois, Urbana-Champaign; M.A., University of Wisconsin.
- ROBERT LINZ, *Head of Public Services and Associate Director of Law Library*. B.A., Wake Forest University; J.D., University of Florida; M.L.I.S., Florida State University.
- 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.

*Adjunct, Adjoint, and Visiting Faculty*

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

BRITT BANKS, *Principal, Nova West LLC*. B.S., University of Denver; J.D. University of Colorado; LLB, University of Colorado.

GEOFFREY BARRY, *Of Counsel, Holland & Hart, Boulder, Colorado*. A.B., Princeton University; J.D., University of Colorado.

GEORGE BRAUCHLER, *Attorney at Law, Caplis & Deasy, LLC, Denver, CO*. B.A., J.D. University of Colorado.

THE HONORABLE ELIZABETH BROWN, *Judge, United States Bankruptcy Court for the District of Colorado*. B.A., Colorado College; J.D. University of Colorado.

JOHN BOYD, *Management/Strategy Consultant*. B.A., University of Iowa; J.D., University of Michigan.

WILLIAM CALLISON, *Partner, Faegre & Benson LLP, Denver, Colorado*. B.A., Oberlin College; J.D., University of Colorado; LL.M., Yale University.

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

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

DARLA DANIEL, *Attorney, Zisman Ingraham & Daniel, Denver, Colorado*. B.A., Trinity University; J.D., University of Colorado.

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

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

BRUCE DIERKING, *Attorney at Law, Boulder, Colorado*. B.A., University of Northern Colorado; J.D., University of Colorado.

THE HONORABLE ALLISON HARTWELL EID, *Justice, Colorado Supreme Court, Denver, Colorado*. A.B., Stanford University; J.D., University of Chicago.

TROY EID, *Shareholder, Greenberg Traurig LLP, Denver, Colorado*. A.B., Stanford University; J.D., University of Chicago.

ERIC ELIFF, *Partner, Morrison Foerster, Denver, Colorado*. B.S., Washington University; J.D., University of Colorado.

ARNOLD ENKER, *Professor of Law, Bar-Ilan University, Israel*. B.A., Yeshiva University; J.D., Harvard University.

JOSEPH FELLER, *Professor of Law, Arizona State University and Senior Counsel for National Wildlife Federation, Boulder, Colorado*. B.A., Harvard University; Ph.D., University of California, Berkeley; J.D., Harvard University.

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

JOHN FRANCIS, *Attorney at Law, Davis Graham & Stubbs, Denver, CO*. B.A., University of Colorado; J.D., University of Michigan Law School.

CRAIG GARBY, *Attorney at Law, Rothgerber Johnson & Lyons LLP, Denver, Colorado*. B.A., University of Colorado; M.P.A., Cornell University; J.D. Stanford University.

THE HONORABLE NEIL M. GORSUCH, *Judge, United States Court of Appeals for the Tenth Circuit, Denver, Colorado*. B.A., Columbia University; J.D., Harvard University; Ph.D., Oxford University.

RANDI GRASSGREEN, *Director of Family Wealth Planning, Crestone Capital Advisors, LLC, Boulder, Colorado*. B.S., University of North Carolina at Chapel Hill; M.T., University of North Carolina at Chapel Hill; J.D., University of Colorado.

LISA GREEN, *Partner, Green and Gardner, LLC, Boulder, Colorado*. B.A., University of Colorado; J.D., University of Cincinnati.

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

ANDREW HARTMAN, *Experiential Learning Program Coordinator & Adjunct Professor, University of Colorado, Boulder, Colorado*. A.B., University of Michigan; J.D., Georgetown University.

KARI HERSHEY, *Shareholder, Hershey Skinner, LLC, Denver, Colorado*. B.A., Michigan State University; J.D. University of Denver.

WILLIAM P. HUNT III, *Adjunct Professor, University of Colorado, Boulder, Colorado*. B.A., University of Missouri Columbia; J.D., Western New England College.

BRUCE KRAMER, *Of Counsel, McGinnis, Lochridge, & Kilgore LLP, Houston, Texas*. B.A., J.D., University of California, Los Angeles; LL.M., University of Illinois.

DAVID KREUTZER, *First Assistant Attorney General, Colorado Attorney General's Office*. B.A., University of Colorado; J.D., University of Denver College of Law.

CHRISTOPHER MCKEE, *Adjunct Professor*. B.A., University of North Carolina, Greensboro; J.D., M.T.S., Emory University.

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

SUSAN MORLEY, *Senior Instructor, University of Colorado Leeds School of Business, Boulder, Colorado*. B.A., University of Kentucky; M.S., University of Colorado; J.D., University of Colorado.

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

PATRICK O'ROURKE, *Managing Associate, University Council, Denver, Colorado*. B.A., Creighton University; J.D., Georgetown University.

PRESTON PADDEN, *Adjunct Professor*. B.A., University of Maryland; J.D., George Washington University.

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

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

THE HONORABLE ROBERT RUSSEL, *Judge, Colorado Court of Appeals, Denver, Colorado*. B.M.E., University of Northern Colorado; J.D., University of Colorado.

PATRICIA J. ROGERS, *Partner, Moye White LLP, Denver, Colorado*. B.A., University of Connecticut; J.D., Georgia State University.

MICHAEL SAUL, *Attorney, Rocky Mountain Natural Resource Center*. B.S., J.D., Yale University.

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

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

*Research Associates*

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

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

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

ADAM REED, *Research Fellow, Center for Energy & Environmental Security*. B.A., Southern Methodist University; J.D., University of Colorado.

JULIE TEEL, *Senior Research Associate, Center for Energy & Environmental Security*. B.S., University of California, Berkeley; J.D., New York University.



## FROM THE EDITOR

Depending on one's faith in technological progress, the Internet and the rise of social media have either permanently obliterated the legal concept of privacy or merely posed new challenges when applying existing law to unforeseen circumstances. Whether or not a truly private life is possible in the age of Google, Facebook, and Twitter, it is clear that traditional notions of privacy law are not equipped to deal with the shift from concerns about intrusive paparazzi to the everyday aggregation of personal information online. Samuel Warren and Louis Brandeis's "right to be let alone" takes on a quaint irony in an era where social media users eagerly broadcast intimate details about their personal lives across the World Wide Web. Nevertheless, the unprecedented ability of computer communications to aggregate personal information and preserve it indefinitely raises serious concerns about discrimination, defamation, and the growing inability to escape the digital record of one's past. Privacy law has yet to recognize the full extent of these challenges and develop new legal tools to resolve them.

In December 2010, the Silicon Flatirons Center at the University of Colorado Law School brought together a distinguished group of privacy scholars, journalists, and industry representatives to debate these issues in the context of modern news reporting. Titled *Privacy and the Press: Scoops, Secrets, and Ethics in the New Media Landscape*, the conference explored issues such as the shifting privacy norms of professional journalism, anonymous commentary and the "unmasking" of abusive online personalities, and the evolving nature of the right to a free press. Thanks to the hard work and influential scholarship of Professor Paul Ohm, this conference on information privacy has been established as an annual tradition at Colorado Law, and we hope that it will contribute to this evolving discipline for years to come.

The *Journal on Telecommunications and High Technology Law* is pleased to publish in this issue five papers presented at the *Privacy and the Press* conference, as well as a variety of scholarship on telecommunications policy, smart grid energy regulation, and consumer genetic testing. Professor Jeffrey Rosen begins the conversation with an overview of the tension between privacy and free speech online, exemplified by the European concept of a "right to oblivion." Professor Neil M. Richards follows with a piece exploring the inadequacy of the Brandeis privacy torts applied to electronic communications. Professor Amy Gajda then warns of the societal danger of allowing privacy regulations to restrict news reporting about crime and the people involved in it. In light of the Internet's promise of viral self-promotion, David Lat and Zach Shemtob discuss the changing definition of a public figure for purposes of defamation law. Professor James Grimmelman

then explores how “first class objects” affect how personal information is represented in computer databases. Professors James Miller and James E. Prieger examine America’s 2009 switch to digital television and the strategic decisions broadcasters made when timing that transition. Silicon Flatirons Fellows J. Pierre de Vries and Kaleb A. Sieh offer a collection of essays on wireless interference compiled from a November 2010 conference in Washington, D.C. Colorado Law student Andreas S. V. Wokutch then proposes a new framework for regulation of smart grid non-utility service providers, and fellow *Journal* editor Angela L. Morrison explores the privacy dangers of consumer genetic testing.

I am grateful to the *Journal’s* editorial board and staff, whose hard work and friendship this year have made countless hours of proofreading and production not only bearable, but one of the best parts of law school. Articles Editors Jennifer McDonald, Shirin Chahal, Angela Morrison, and Meredith Simmons deserve credit for their thoughtful editorial work on each article in this issue, and Production Editors Therese Kerfoot and Jake Adkins have my sincere thanks for their attention to detail and commitment to seeing the publication process through to the end. Managing Editor Alison Jensen excelled at planning the *Journal’s* budget and social events, Executive Editor Catherine Holtgrewe ensured that staff members received well-deserved academic credit for their work, and Resource Editor Christian Alexander kept cite checks on schedule by diligently locating obscure source materials. Student Note Editors Kimberly West, Desta Asfaw, Kazuyo Morita, Rebecca Siska-Salkin, and Angela Wade each worked closely with student authors, inspiring an impressive range of scholarship that we are pleased to recommend for publication in the next volume of the *Journal*. Associate Editors Vlad Etinger, Tawnya Ferbiak, and Christine Rinke also proved invaluable in helping keep the production process on track. I appreciate the efforts of the entire staff to bring this issue to press, but Symposium Editor Madelaine Maior and Associate Symposium Editor Janna Fischer also deserve special commendation for their hard work. I am proud of what we all accomplished this year and am confident that the best is yet to come as the *Journal* reaches the upcoming milestone of its tenth volume.

I thank the Colorado Law faculty and the Silicon Flatirons Center for their support of the *Journal* and helpful guidance throughout the year. We are fortunate to have many trusted mentors such as Professors Phil Weiser, Dale Hatfield, Brad Bernthal, Preston Padden, and Andy Hartman, and it has been a pleasure to work with Anna Noschese, Jamie Stewart, and the rest of the Silicon Flatirons staff. I also am grateful to journal manager Martha Utchenik for her wealth of institutional knowledge and personal dedication to the *Journal*, as well as to the members and editors of the *University of Colorado Law Review* and the *Colorado Journal of International Environmental Law and Policy* for their cooperation and collegiality.

Finally, I am pleased to dedicate this issue to Professors Paul Ohm and Harry Surden, who as faculty advisors to the *Journal* have opened their minds, offices, and e-mail inboxes to more questions, comments, and frantic pleas for assistance than I can count. Their wise counsel and generosity with their own time and expertise has made editing this journal a valuable learning experience on both an academic and a personal level. I admire Professor Ohm's ambition in expanding the *Journal's* focus into the information privacy field and particularly appreciate his efforts this year to bring that goal to fruition. With bright and capable members and editors, forward-thinking advisors, and some of the most thought-provoking scholarship in the technology and telecommunications fields, the *Journal on Telecommunications and High Technology Law* is truly something special, and it has been an honor to be a part of it.

*Eric P. Schmidt*  
*Editor-in-Chief*



# CONTENTS

## INFORMATION PRIVACY

|  |     |
|--|-----|
| FREE SPEECH, PRIVACY, AND THE WEB THAT NEVER FORGETS<br><i>JEFFREY ROSEN</i> ..... | 345 |
| THE LIMITS OF TORT PRIVACY<br><i>NEIL M. RICHARDS</i> .....                        | 357 |
| THE VALUE OF DETECTIVE STORIES<br><i>AMY GAJDA</i> .....                           | 385 |
| PUBLIC FIGUREHOOD IN THE DIGITAL AGE<br><i>DAVID LAT &amp; ZACH SHEMTOB</i> .....  | 403 |
| FIRST-CLASS OBJECTS<br><i>JAMES GRIMMELMANN</i> .....                              | 421 |

## TELECOMMUNICATIONS

|  |     |
|--|-----|
| THE BROADCASTERS' TRANSITION DATE ROULETTE:<br>STRATEGIC ASPECTS OF THE DTV TRANSITION<br><i>JAMES MILLER &amp; JAMES E. PRIEGER</i> ..... | 437 |
| THE UNFINISHED RADIO REVOLUTION:<br>EIGHT PERSPECTIVES ON WIRELESS INTERFERENCE<br><i>J. PIERRE DE VRIES &amp; KALEB A. SIEH</i> .....     | 501 |

## ENERGY REGULATION

|  |     |
|--|-----|
| THE ROLE OF NON-UTILITY SERVICE PROVIDERS IN SMART<br>GRID DEVELOPMENT: SHOULD THEY BE REGULATED,<br>AND IF SO, WHO CAN REGULATE THEM?<br><i>ANDREAS S. V. WOKUTCH</i> ..... | 531 |
|--|-----|

## STUDENT NOTE

|  |     |
|--|-----|
| A RESEARCH REVOLUTION: GENETIC TESTING CONSUMERS<br>BECOME RESEARCH (AND PRIVACY) GUINEA PIGS<br><i>ANGELA L. MORRISON</i> ..... | 573 |
|--|-----|



# FREE SPEECH, PRIVACY, AND THE WEB THAT NEVER FORGETS

BY JEFFREY ROSEN\*

Thank you so much and good morning. It is a great pleasure to be here. As Paul Ohm said, my interest in the fascinating subject of how to reconcile free speech and privacy, in an age when the Web never forgets, began with a conversation that we had about a year ago. Paul's work—and the center he's established here—have been invaluable in exploring the tensions between free speech and privacy on the Internet, and I can't think of a better place to talk about these challenging issues. So I am much looking forward to our conversation.

Keynote address sounds a little grand, but I'm at least supposed to set the stage for our discussions. And, what I want to say is this: new media technologies are presenting wrenching tensions between free speech and privacy. Around the world citizens are experiencing the difficulty of living in a world where the Web never forgets, where every blog and tweet and Facebook update and MySpace picture about us is recorded forever in the digital cloud. This experience is leading to tangible harms, dignitary harms, as people are losing jobs and promotions. But—and this is a big “but”—law is not always a good remedy for these harms. Although there are proposals in Europe and around the world to create new legal rights of oblivion that would allow us to escape our past, these rights pose grave threats to free speech.<sup>1</sup> And if forced to choose between my privacy instincts and my free speech instincts, I have no hesitation in this case in choosing free speech over privacy. So if there are to be remedies for the problem of digital forgetting, my sense is that the most promising ones involve technology and norms and not law.

Let's begin with a reluctant icon of the problem of digital forgetting, because it's hard to talk about a privacy problem without putting a face to it. The privacy icon that is bringing home to people the

---

\* Jeffrey Rosen is a professor of law at The George Washington University and the legal affairs editor of The New Republic. He the author of *The Supreme Court: The Personalities and Rivalries that Defined America*, *The Most Democratic Branch*, *The Naked Crowd*, and *The Unwanted Gaze*. Rosen is a graduate of Harvard College, *summa cum laude*; Oxford University, where he was a Marshall Scholar; and Yale Law School.

1. See *infra* notes 36 & 43-46 and accompanying text.

dangers of a Web that never forgets is Stacy Snyder. She is the young woman who was about to graduate from teachers college, and days before her graduation her employer, a public high school, discovered that she had posted on MySpace a posting criticizing her supervising teacher and a picture of herself with a pirate's hat and a plastic cup and she had put the caption "drunken pirate" under it.<sup>2</sup> The school concluded that she was behaving in an unprofessional way and promoting underage drinking. Therefore, they did not allow her to complete her student teaching practicum.<sup>3</sup> As a result, her teachers college denied her a teaching certificate.<sup>4</sup>

She sued and invoked the First Amendment, claiming she had a free speech right to post the MySpace picture.<sup>5</sup> A federal judge rejected her claim on two grounds.<sup>6</sup> He said, first, that she was a public employee and, second, that her speech did not relate to a matter of public concern.<sup>7</sup> Because Snyder lost her lawsuit, she never graduated from teachers college, and she is now working in human resources.<sup>8</sup>

The unfortunate case of Stacey Snyder sums up the problem of what to do when we've posted embarrassing information about ourselves and have trouble getting it back down. Claiming we have a free speech right doesn't work under American law. Nor could she attempt to claim that she has a constitutional privacy right against MySpace, a private corporation.

If Stacey Snyder were in Europe, she might claim that her dignitary rights had been assaulted, and she might demand that Google and Yahoo remove all references to the picture by invoking a new right proposed by the European Union and the French data protection President, namely a right to oblivion.<sup>9</sup> This is an extremely French notion. In America we want to be remembered; the French want to be forgotten. It's straight out of Sartre. And the French data protection President, Alex Türk, has proposed that you should be able to remove embarrassing information about yourself.<sup>10</sup> Google and Yahoo should not be allowed to index the picture even if they want to, and they should

2. Snyder v. Millersville Univ., 2008 U.S. Dist. LEXIS 97943 (E.D. Pa., Dec. 3, 2008).

3. *Id.* at \*6-8.

4. *Id.* at \*8-9. Instead of receiving a Bachelor of Science with a teaching certificate, Snyder graduated with a Bachelor of Arts in English. *Id.* at \*2.

5. *Id.* at \*15-16.

6. *Id.*

7. *Id.* at \*16.

8. Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG., July 21, 2010, at MM30.

9. *Data Protection Reform – Frequently Asked Questions*, EUROPA, Nov. 4, 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/542&format=HTML&aged=0&language=EN&guiLanguage=en> (last visited May 13, 2011).

10. *Id.*

have to pay you damages if they index the picture in ways that cause you moral harm. Now this obviously raises tremendous free speech implications. I had a good debate with the French data protection President<sup>11</sup> in Jerusalem at a recent privacy conference,<sup>12</sup> and I asked about the details of how the right to oblivion would to be implemented. Well, he suggested, you would need an international tribunal of forgetfulness to adjudicate on a case-by-case basis what pictures had to come up and what came down. Who would decide what was worthy and what was free speech? “Well, experts would decide this sort of thing.”

This is an area where Europe and America very much diverge, and I’m curious to take a pulse of the audience right now. If forced to choose right now, without more details, would you endorse a legally enforceable right to oblivion or do you prefer the free speech side? Who would choose the right to oblivion? And who would prefer free speech? I’m not surprised to see such a strong majority for speech. That’s the American way.

Stacy Snyder may be the modern icon, but obviously this is not a new problem. It goes back to Brandeis. You’ll forgive me for proselytizing, but I am writing about the relevance of Louis Brandeis today, and when it comes to the tension between free speech and privacy, Brandeis is both our greatest prophet of protecting privacy in an age of new technologies and of protecting free speech in an age of expanding democracy. How would he come down on the tension between two liberties he cared passionately about?

Brandeis’s famous article on the right to privacy in 1890, of course, was reacting to a particular technology, the instant camera and the tabloid press.<sup>13</sup> He said they ensured that what once was whispered in the closets was now shouted from the rooftops.<sup>14</sup> “To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers[,]” he wrote. “To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.”<sup>15</sup> The item that upset Brandeis is conventionally said to have been a mild society item in the Boston tabloids about

11. Alex Türk is the president of France’s National Commission on Informatics and Liberties. *Alex Türk – President of CNIL*, NAT’L COMM’N ON INFORMATICS AND LIBERTIES (CNIL), <http://www.cnil.fr/la-cnil/qui-sommes-nous/equipes/la-commission/alex-turk> (last visited Apr. 20, 2011).

12. The 32nd Annual Conference of Data Protection and Privacy Commissioners was held October 27, 2010, in Jerusalem, Israel. *See* 32ND INT’L CONFERENCE OF DATA PROT. & PRIVACY COMM’RS, <http://www.justice.gov.il/PrivacyGenerations> (last visited Apr. 20, 2011).

13. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

14. *Id.*

15. *Id.* at 196.

Brandeis's partner's daughter's wedding breakfast.<sup>16</sup> This can't have been the case, because as Brandeis's biographer, Melvin Urofsky, said, the daughter was only a few years old at the time.<sup>17</sup> But Brandeis himself said that Samuel Warren, his co-author, was concerned about the intrusions on social privacy by the tabloid press.<sup>18</sup> As a result of these intrusions, Brandeis proposed the four Brandeis torts, which sounds like a yummy dessert.<sup>19</sup> But they proved in practice, for reasons Neil Richards will explore today, to have been an inadequate way of protecting privacy in an age of new technology.<sup>20</sup>

The reasons that the Brandeis torts largely failed are, first, because they pose grave threats to free speech and require decisions about who is a public figure and who is not—a concern that, as David Lat will describe, is more and more difficult in an age when everyone has his or her 15 minutes and everyone is a micro public figure with a few Twitter followers. *The New York Times* reported on a 26-year-old Manhattan woman who said that she is afraid of going out on dates and being tagged in online photos because it would reveal that she only wears two outfits.<sup>21</sup> “You have movie star issues,” she said, “and you’re just a person.”<sup>22</sup>

In Brandeis's day you had to be a Boston aristocrat to be gossiped about in the tabloids, and now all of us are experiencing the indignity of being tagged and commented on. Trying to identify who is a public figure and who is not is increasingly elusive. So, that is one reason the Brandeis torts failed, and it's all the more difficult now that the scope of people who are being commented on has so dramatically increased. Brandeis and Warren were concerned about a few Boston tabloids; now Facebook has more than 500 million members who share more than 30 billion pieces of content a month.<sup>23</sup> The sheer scope of the gossip is so extreme that the idea that law could constrain it is more implausible than ever.

Another reason the Brandeis torts failed is because they all depend on some social consensus about what sort of invasions are highly offensive to a reasonable person or outrageous according to existing social

16. Dorothy Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979) (citing Letter from Roscoe Pound to William Chilton (1916), in ALPHEUS THOMAS MASON, *BRANDEIS: A FREE MAN'S LIFE* 70 (1956)).

17. *Id.* at 5 (citing William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383-84, 423 (1960)).

18. *Id.* at 6 (citing MASON, *supra* note 16, at 70).

19. Warren & Brandeis, *supra* note 13, at 214-18.

20. See Neil M. Richards, *The Limits of Tort Privacy*, 9 J. ON TELECOMM. & HIGH TECH. L. 357 (2011).

21. Rosen, *supra* note 8, at MM30.

22. *Id.*

23. *Statistics*, FACEBOOK, <https://www.facebook.com/press/info.php?statistics> (last visited Apr. 16, 2011).

norms. And, as sexual mores changed, as gender equality grew, juries and citizens could no longer agree about what sort of intrusions were highly offensive—a problem that’s only exacerbated by the volume of content on the Web.

There has also been a transformation in the idea of gossip itself and of its status in our society. Gossip is conventionally defined as idle talk about the personal or private affairs of others.<sup>24</sup> I am not concerned right now about rumors, which may be false. I want to focus on truthful, but embarrassing, private gossip about the personal affairs of others. In Brandeis’s day, Brandeis lamented the idea that a focus on private matters could crowd out the attention in the public sphere that could be devoted to matters of public concern. “Easy of comprehension, appealing to that weak side of human nature which is never wholly cast down by the misfortunes and frailties of our neighbors, no one can be surprised that it usurps the place of interest in brains capable of other things,”<sup>25</sup> he wrote. Today, we lack that confidence about the importance of maintaining the boundaries between higher and lower discourse. Now the personal is political; authenticity is more important than reticence, and disclosure norms are being transformed. Talk about private affairs, from Eliot Spitzer to the Duke lacrosse players, is inherently considered a matter of public concern, and we do not want judges deciding in advance what people should be interested in.<sup>26</sup> So the idea that off-the-record conversations, as these WikiLeaks show so dramatically, shouldn’t be attended to in the public sphere is not something that we are willing to accept.

There is yet another difference between Brandeis’s day and ours that makes the idea of the Brandeis torts hard to enforce. And that’s the end of the distinction between oral and written gossip. E.L. Godkin wrote an article on gossip just around the time that Brandeis wrote his famous article, and emphasized that oral gossip was less of a dignitary harm because it didn’t have to be responded to; it didn’t assault your public face if you knew your neighbors were gossiping about you behind your back.<sup>27</sup>

By contrast, once something was written down in the press it

---

24. See, e.g., NEW OXFORD AMERICAN DICTIONARY 750 (3d ed. 2010) (defining gossip as “casual or unconstrained conversation or reports about other people . . . a person who likes talking about other people’s private lives”).

25. Warren & Brandeis, *supra* note 13, at 196.

26. See Danny Hakim & William K. Rashbaum, *Spitzer is Linked to Prostitution Ring*, N.Y. TIMES (Mar. 10, 2008), <http://www.nytimes.com/2008/03/10/nyregion/10cnd-spitzer.html?pagewanted=all>; Duff Wilson, *Lawyer Says Two Duke Lacrosse Players Indicted in Rape Case*, N.Y. TIMES, Apr. 18, 2006, at A23.

27. E.L. Godkin, *The Rights of the Citizen: IV. To His Own Reputation*, 8 SCRIBNER’S MAG. 58, 66 (1890).

required a response. Facebook has literally exploded that distinction, and gossip that used to be spoken is now written down and has to be responded to, a transformation that is also challenging the distinction between the low and high press. It used to be, even during the Clinton era, that if something was in the *National Enquirer*, you didn't have to respond to it, but if it was in *The New York Times*, you did. Now the *National Enquirer* itself is breaking sex stories of political significance, such as Al Gore's poodle-like indiscretions,<sup>28</sup> and the idea that there is a distinction between the *Enquirer* and the *Times* is under stress. In other words, the Brandeis torts were on life support even before the explosion of the Internet. The 'Net has only added increasing pressure that makes it hard to resurrect them.

In the U.S., as a result of these pressures, we've drawn what I think is a fairly sensible legal line which is that very little truthful but embarrassing speech is actionable. Only outrageous sexual surveillance in its most pristine form—hidden cameras of sexual activity—is actionable, but little else is. The Rutgers suicide case is a good example here of the kind of privacy invasion that almost everyone thinks should be actionable.<sup>29</sup> This is the tragic case of the young Rutgers student whose roommate turned on a Webcam in their shared dorm and live-broadcasted his dorm room intimacies.<sup>30</sup> The young man was so upset that days later he committed suicide.<sup>31</sup> The roommate and an accomplice are being charged under New Jersey law, and everyone expects them to get serious jail time.<sup>32</sup> Rutgers students are debating whether a five year sentence is too harsh, but few people are disputing that extreme sexual surveillance should be actionable.

What about sexual surveillance in written form, by the blogosphere rather than by the cameras? Here the paradigm case is "the Washingtonienne."<sup>33</sup> A few years ago a blogger, Jessica Cutler, a Capitol Hill staffer for a Republican senator, chronicled her sexual experiences with six different men whom she identified by initials and in some cases by name, including details of their performances and proclivities.<sup>34</sup> One of them, Robert Steinbuch, a fellow staffer, sued Cutler as well as

---

28. *Al Gore Sex Scandal*, NAT'L ENQUIRER (June 29, 2010, 11:00 PM EDT), <http://www.nationalenquirer.com/celebrity/new-evidence-revealed-gore-sex-scandal-victim-tells-all>.

29. Lisa W. Foderaro, *Private Moment Made Public, Then a Fatal Jump*, N.Y. TIMES, Sept. 30, 2010, at A1.

30. *Id.*

31. *Id.*

32. *Id.* (Both were charged with two counts of "invasion of privacy"; the most serious charge has a maximum penalty of five years in prison).

33. See Dan Glaister, *Washington Gets Ready to Gossip as DC Sex Blog Goes to Court*, GUARDIAN, Dec. 28, 2006, at 21.

34. *Id.*

Hyperion, which published the inevitable tell-all book that followed.<sup>35</sup> In 2006, a district judge refused to dismiss the lawsuit against Cutler, who went bankrupt, and the Eighth Circuit refused to dismiss the lawsuit against Hyperion.<sup>36</sup> Two years later, the publisher settled with Steinbuch.<sup>37</sup> This shows how hard it is to recover for privacy invasions that are quite dramatic. Had the case gone to trial, Steinbuch might have lost. Was Steinbuch a public figure or not? Was the blog widely circulated? Was the speech a matter of public concern? All of that might have come out at trial, but because of the dangers of litigation the publishers settled and Steinbuch feels vindicated. He is now a law professor at the University of Arkansas,<sup>38</sup> but clearly lawsuits are not a meaningful remedy for most people without very strong stomachs, if not deep pockets. So that's the American line: sexual surveillance by camera or possibly in blogs is possibly actionable, but very little else is, and I think that's a very good legal line to draw that respects free-speech values.

What are alternatives? As I said, other countries are exploring different models that would create legally enforceable rights to forgetting, and the harbinger here is Argentina. Argentina has no fewer than 130 cases pending to force search engines to remove or block offensive content.<sup>39</sup> The leading case about the right to forgetting in Argentina involves a pop star called Virginia da Cunha.<sup>40</sup> She was the lead singer of a band called Bandana who indiscreetly took some racy pictures of herself voluntarily, and they were posted online.<sup>41</sup> After the fact, she thought the better of these pictures and decided that, although she had posed for them voluntarily, they affronted her moral dignity.<sup>42</sup> A judge agreed that there was a dignitary offense to having these pictures out there, and the judge ordered Google and Yahoo to pay 50,000 pesos each in damages simply because their search results had included pictures

---

35. *Id.*; JESSICA CUTLER, *THE WASHINGTONIENNE: A NOVEL* (2005).

36. *Steinbuch v. Cutler*, 2006 U.S. Dist. LEXIS 19025 (D.D.C. Apr. 14, 2006) (denying Cutler's motion to dismiss); *Steinbuch v. Cutler*, 518 F.3d 580 (8th Cir. 2008) (reversing dismissal against Hyperion).

37. Jeffrey Rosen, *Privacy Strikes Back - How to Stop Cyber-Bullies*, NEW REPUBLIC, Nov. 11, 2010, at 6.

38. *Bio: Robert Steinbuch*, UNIV. OF ARK. AT LITTLE ROCK WILLIAM H. BOWEN SCH. OF LAW, <http://www.law.ualr.edu/faculty/bios/steinbuch.asp> (revised Aug. 17, 2010).

39. *Yahoo! Declared Not Liable for Defamation in Argentina*, YAHOO! BUS. & HUM. RTS. (Aug. 26, 2010, 9:43 PM), <http://www.yhumanrightsblog.com/blog/2010/08/26/yahoo-declared-not-liable-for-defamation-in-argentina/>.

40. *See generally* Vinod Srecharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES, Aug. 20, 2010, at B4.

41. *See generally* Lance Whitney, *Google, Yahoo Win Argentine Celebrity Search Case*, CNET NEWS (Aug. 20, 2010, 11:58 AM PDT), [http://news.cnet.com/8301-13578\\_3-20014265-38.html](http://news.cnet.com/8301-13578_3-20014265-38.html).

42. *Id.*

of Da Cunha that were linked to erotic content.<sup>43</sup> Yahoo said that the only way to comply with the injunctions would be to block all sites that refer to a particular plaintiff.<sup>44</sup> That might be feasible in a Google situation where there is a country-specific website like Google Argentina.<sup>45</sup> But Yahoo is now using Bing<sup>46</sup>—which may only have one platform—so to block references to this pop star on Bing means all references to her would turn up no search result.

This strikes me as an Orwellian vision of rewriting history on a selective basis. And you can imagine all sorts of cases where the pop star might have decided to run for office, as European porn and pop stars tend to do, became embarrassed about the search results, and then demanded that all references to herself be blocked because of her interest in escaping her past.

My First Amendment knee jerked at this, but I was struck to see how seriously Europe is debating creating broad rights of oblivion. Not only Alex Türk, but Viviane Reding, the European minister for justice and civil rights, has proposed a right to be forgotten that would require a search engine to ignore tagged results.<sup>47</sup> There's another EU proposal to create a legal right to disappearing data,<sup>48</sup> raising all sorts of legal questions. Would the user's right be against Facebook to delete the information that he wrote on his Facebook account? If so, would the same right apply when a third-party Facebook user copied and forwarded the information? Would we need a new definition of data ownership? The details of implementing this right would be complicated, in addition to posing lots of free-speech problems. There may be a big conflict between Europe and America. And we, as privacy and free-speech scholars, will have to debate vigorously where to draw the lines.

There are other proposals in the U.S. to expand the tort and contractual remedies for dignitary invasions. My colleague at George Washington, Daniel Solove, proposes expanding breach of confidence

43. Sreeharsha, *supra* note 41; Juzgado Nacional de Primera Instancia [1a Inst.], 29/7/2009, "Da Cunha Virginia c. Yahoo de Argentina SRL y otro s/ Daños y perjuicios", No. 75, Expte. No. 99.620/06) (Arg.).

44. Sreeharsha, *supra* note 41.

45. See Google Argentina, <http://www.google.com.ar> (last visited Apr. 17, 2011).

46. Nancy Gohring, *Yahoo Moves to Bing in North America*, REUTERS (Aug. 24, 2010, 8:43 AM EDT), <http://www.reuters.com/article/2010/08/25/urnidgns852573c40069388088257789006eb-idUS129778380120100825>.

47. Leigh Phillips, *EU to Force Social Network Sites to Enhance Privacy*, GUARDIAN (Mar. 16, 2011, 17:38 GMT), <http://www.guardian.co.uk/media/2011/mar/16/eu-social-network-sites-privacy>.

48. Jason Walsh, *When it Comes to Facebook, EU Defends the "Right to Disappear"*, CHRISTIAN SCI. MONITOR (Apr. 6, 2011), <http://www.csmonitor.com/World/Europe/2011/0406/When-it-comes-to-Facebook-EU-defends-the-right-to-disappear>.

suits so you could sue your Facebook friends for breaching confidence if they violate your privacy settings.<sup>49</sup> That would keep the plaintiffs' bar very busy, in my view. And the practical difficulties of suppressing that volume of speech concern me, as well as the free-speech issues, which are complicated. My instinct in all of these cases is that law is too heavy-handed an instrument and technological solutions are better.

So the solution I like best is proposed by Viktor Mayer-Schönberger in his wonderful book "Delete." That solution is expiration dates for data.<sup>50</sup> Facebook could, if it chose, encourage the development of apps that would allow us, when we post that drunken picture from Cancun, to specify whether we want the picture to stay up there forever or for three months or for three days. And Google, of course, now has an app that asks you when you post e-mails at midnight on Saturday when you may be tipsy, "are you sure you really want to do this?"<sup>51</sup> The combination of persuasive technologies like that combined with a specification that the picture should only last for three days when it's posted on a Saturday evening would go a long way toward solving the problem.

Facebook has been reluctant to encourage these apps at the moment because of its business model, which encourages it asserting ownership over its data and targeting apps on the basis of it. But I think that soft nudges from privacy regulators, not creating a legal right to delete, but creating incentives to develop apps that would allow this, would be welcome.

A small-scale model of this is TigerText, which is the text messaging system that allows you to say that you want your texts to disappear after three months or three days.<sup>52</sup> (This was named before the Tiger Woods text-messaging scandal.) And a new German Facebook app, X-Pire, would also create an option of disappearing data.<sup>53</sup> We need more apps along these lines, and more support for them from the Facebook platform.

In addition to technological solutions, there are norms-based solutions. The Japanese have come up with a great solution along these lines. In Japan, social networking accounts are almost always pseudonymous.<sup>54</sup> People rarely use their real names, so if your real friend

49. DANIEL J. SOLOVE, *PRIVACY IN AN OVEREXPOSED WORLD* 174-76 (2007).

50. VIKTOR MAYER-SCHÖNBERGER, *DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE* 15 (2009).

51. See Jon Perlow, *New in Labs: Stop Sending Mail You Later Regret*, GMAIL OFFICIAL BLOG (Oct. 6, 2008, 6:25 PM), <http://gmailblog.blogspot.com/2008/10/new-in-labs-stop-sending-mail-you-later.html> (describing how Mail Goggles requires users during late-night weekend hours to solve math problems before an email will send).

52. See TIGERTEXT: SECURE MOBILE MESSAGING, <http://www.tigertext.com> (last visited Apr. 17, 2011).

53. See X-PIRE, <http://www.x-pire.de/index.php?id=6&L=2> (last visited Apr. 17, 2011).

54. Hiroko Tabuchi, *Facebook Wins Relatively Few Friends in Japan*, N.Y. TIMES, Jan. 10, 2011, at B1 (stating, "[i]n a survey of 2,130 Japanese mobile Web users . . . , 89 percent of

is someone who is not a fake friend, you share your pseudonym. That way, your real friends have access to the whole account, but employers and strangers never do, and you can always walk away from your pseudonym. That kind of pseudonymity is more practical than Google CEO Eric Schmidt's solution: people should just change their names on high school graduation.<sup>55</sup>

The question of norms and gossip brings us to perhaps the most practical solution to the problem of digital forgetting, which is to create new norms of atonement and forgiveness. The Talmud, for example, takes gossip very seriously, and it prohibits *lashon hara*, which includes not only false gossip or tale bearing, but even truthful tale bearing or speech about others, unless the gossip has a serious public purpose.<sup>56</sup> Every word that we speak, according to the Talmud, ascends to the divine cloud, and Google's virtual cloud has made this metaphor literal. The Talmud says that the only way to atone for speech about others—even if it's the truth and not especially nasty—is to go to the person that you have spoken about and ask for forgiveness. But if the person you've gossiped about forgives you for the gossip, then God wipes the heavenly slate clean.<sup>57</sup> The idea in the Talmud that you can atone for your mistakes allows the possibility not only of forgetfulness, but of forgiveness, which allows us to grow in wisdom and to become better people and atone for our sins. The Talmud says, "Let it not be said of a repentant sinner 'remember your former deeds.'"<sup>58</sup> It is a terrible sin to call someone to account for bad deeds in the past if they have been atoned for.

What can these rituals of atonement and forgiveness teach us as journalists about gossip? I think Paul and Wendy Seltzer's paper is a model in this regard. As you'll see, they have a concrete recommendation: that media outlets should not publish stories based solely on leads developed through non-public social networking sites.<sup>59</sup> They describe Facebook chat as the equivalent of water cooler gossip, which in fact it is. People share gossip on Facebook, not intending for it to be fully public. And if journalists respected that and didn't quote from it directly, they could set privacy norms and help construct zones of privacy. Journalists can follow these sorts of norms. In the *Times*

---

respondents said they were reluctant to disclose their real names on the Web.").

55. Holman W. Jenkins, Jr., *Google and the Search for the Future*, WALL ST. J., Aug. 14, 2010, at A9.

56. Leviticus 19:16.

57. TALMUD, Baba Mezi'a 58b.

58. *Id.*

59. See Privacy and the Press: Scoops, Secrets, and Ethics in the New Media Landscape, *Panel One: The Shifting Privacy Norms of Journalism*, SILICON FLATIRONS (Dec. 3, 2010), <http://lawweb.colorado.edu/events/mediaDetails.jsp?id=3164>.

*Magazine* piece, as it happens, I quoted an interview with a Texas scholar that took place on a public Facebook privacy blog, and that seemed to me fair game.<sup>60</sup> But quoting that scholar's own Facebook chat would seem like a very different kettle of fish.

As for piercing anonymity, I'm suspicious of it on free-speech grounds unless the harm caused by the anonymous speech is clearly and indisputably illegal under current law. Anonymity is necessary to encourage the expression of unpopular opinions, especially in this age of digital mobs where conformity is so quickly and so brutally enforced. It's also a norm to comment anonymously, as the comments section on any news article will show. It can be harrowing as a journalist to be dissected anonymously, but it's very much a part of a vigorous free-speech debate, and as the Supreme Court recognized in the NAACP case where it refused to require the NAACP to turn over its membership lists, the piercing of anonymity can have huge chilling effects.<sup>61</sup>

Where does this leave us? We have a raucous new universe where there is less and less distinction between spoken and written gossip or between public and private speech. Anonymity reigns, and there are harsh attacks without obvious legal remedies. But as Louis Brandeis recognized better than anyone, democracy is not for the faint-hearted.<sup>62</sup> And when I wonder what Brandeis would have made of the blogosphere, I imagine he would have been nervously optimistic about its potential, even as he recognized its dangers. He would have been appalled by the polarization of speech on the Internet, by the explosion of trivial gossip. But ultimately he was an optimist. I imagine he would have recognized that to the degree the Web is expanding the opportunities for ordinary citizens to debate both public and private issues in chat rooms and other virtual spaces, this is a fulfillment of the highest free-speech ideal which Brandeis located in Periclean Athens and in the shires of Jeffersonian democracy. Small-scale communities that allow vigorous Web debates were his ideal.

When I wonder about how Brandeis would have resolved conflicts between privacy and free speech, I imagine he would have come down on the side of free expression. He was the inventor of the idea that sunlight is the best disinfectant, and his concurring opinion in *Whitney v. California* is the greatest and most inspiring essay on free speech ever written in the 20th century.<sup>63</sup> And here's what Brandeis said:

---

60. Rosen, *supra* note 8, at MM30.

61. NAACP v. Patterson, 357 U.S. 449, 458 (1958).

62. *Whitney v. California*, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

63. *Id.*

Those who won our independence by revolution were not cowards. They did not fear political change. They did not exalt order at the cost of liberty. To courageous, self-reliant men, with confidence in the power of free and fearless reasoning applied through the processes of popular government, no danger flowing from speech can be deemed clear and present, unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion. If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence. Only an emergency can justify repression. Such must be the rule if authority is to be reconciled with freedom. Such, in my opinion, is the command of the Constitution.<sup>64</sup>

That's my opinion, too, and I look forward to our conversation about these fascinating issues. Thank you so much.

---

64. *Id.*

# THE LIMITS OF TORT PRIVACY

NEIL M. RICHARDS\*

The conception of tort privacy developed by Warren, Brandeis, and Prosser sits at the heart of American understandings of privacy law. Rooted in protection of private information against unwanted collection, use, and disclosure, tort privacy protects against emotional injury and was directed by design against disclosures of true, embarrassing facts by the media. In this essay, I argue that as conceived by Samuel Warren and Louis Brandeis and interpreted by William Prosser, tort privacy is a poor vehicle for grappling with problems of privacy and reputation in the digital age. Tort privacy, especially the disclosure tort, has from its inception been in conflict with First Amendment values. And when First Amendment values and tort privacy conflict, First Amendment values should prevail virtually all of the time. The disclosure tort will retain limited utility in the electronic environment, but privacy in the age of information and social media requires new strategies and new legal tools. Some of these strategies might include tort privacy as presently understood, but others require new approaches. These approaches can take either a broader look at tort privacy, including new torts and new theories of injury beyond emotional harm, or they can include new conceptions of privacy altogether, such as confidentiality law.

|   |     |
|---|-----|
| INTRODUCTION.....                                     | 358 |
| I. THE ORIGINS AND THEORY OF TORT PRIVACY.....        | 361 |
| II. DISCLOSURE AND THE FIRST AMENDMENT CRITIQUE ..... | 365 |
| III. THE LIMITS OF DISCLOSURE .....                   | 374 |
| CONCLUSION: RETHINKING INVASION OF PRIVACY.....       | 382 |

---

\* Professor of Law, Washington University School of Law. An early draft of this essay was presented at the Silicon Flatirons Conference on Privacy and the Press at the University of Colorado on December 4, 2010. For helpful comments and conversations about the ideas in this paper, thanks to Danielle Citron, Rick Garnett, Mark McKenna, Paul Ohm, Paul Schwartz, Dan Solove, and my Silicon Flatirons co-panelists Sandra Barron, David Lat, Helen Norton, and Steven Zansberg. Thanks also to participants in workshops at Notre Dame Law School and Berkeley Law School. Special thanks to Eric Schmidt and to Jim Stanley for outstanding research assistance.

## INTRODUCTION

On September 19, 2010, Rutgers College freshman Darun Ravi used a webcam to covertly record a video of his roommate Tyler Clementi having sex with another student.<sup>1</sup> Ravi boasted about the incident on Twitter and attempted to record another of Clementi's sexual encounters two days later, inviting his Twitter followers to view streaming video of the sequel as an Internet event.<sup>2</sup> Ravi was apparently assisted in these actions by Molly Wei, a hallmate.<sup>3</sup> On September 22, apparently as a result of the torment caused by these events, Clementi jumped to his death from the George Washington Bridge.<sup>4</sup> Although it is not known whether Clementi's sexual orientation was a contributing factor in Ravi and Wei's decisions to target him, the incident helped prompt a national debate about harassment of young people on the basis of their sexuality and prompted the highly successful "It Gets Better Project" in support of gay youth.<sup>5</sup> Ravi and Wei have been charged under New Jersey law with criminal invasion of privacy and transmission of the recording of a sexual act.<sup>6</sup> It is likely that civil actions for invasions of privacy will be brought by Clementi's family and estate.<sup>7</sup>

On January 25, 2011, Egyptian dissidents opposed to President Hosni Mubarrak began a series of protests in Taksim square, using social media platforms like Twitter and Facebook to encourage attendance at their gatherings and keep readers around the world informed about their situation.<sup>8</sup> In response, the Mubarak government attempted to shut off

1. Lisa Fodararo, *Private Moment Made Public, Then a Fatal Jump*, N.Y. TIMES, Sept. 30, 2010, at A1.

2. *Id.*

3. *Id.*

4. *Id.*

5. See, e.g., Lisa Fodararo & Winnie Hu, *Online Musings Point to Student's State of Mind Before a Suicide*, N.Y. TIMES, Oct. 1, 2010, at A17; Sean Gardiner & Alison Fox, *Grief, Outrage at Rutgers*, WALL ST. J., Oct. 2, 2010, at A19; Brad Knickerbocker, *Tyler Clementi Suicide: Reaction Is Swift and Widespread*, CHRISTIAN SCI. MONITOR, Oct. 3, 2010, available at <http://www.csmonitor.com/USA/Society/2010/1003/Tyler-Clementi-suicide-Reaction-is-swift-and-widespread>; Kathleen Parker, *With Tyler Clementi's Death, Let's Try Friending Decency*, WASH. POST, Oct. 3, 2010, at A19; John Schwartz, *Bullying, Suicide, Punishment*, N.Y. TIMES, Oct. 2, 2010, at WK1. The "It Gets Better Project" videos are hosted at [www.itgetsbetter.org](http://www.itgetsbetter.org).

6. Winnie Hu, *Legal Debate Swirls Over Charges in a Student's Suicide*, N.Y. TIMES, Oct. 2, 2010, at A15; Geoff Mulvihill & Samantha Henry, *N.J. Gay Video Suicide Case May Result in Bias Charges*, ST. LOUIS POST-DISPATCH, Oct. 1, 2010, at A23; Jeffrey Rosen, *Privacy Strikes Back*, NEW REPUBLIC, Nov. 11, 2010, at 5.

7. Nate Schweber, *Parents of Student Who Committed Suicide Tell Rutgers University They May Sue*, N.Y. TIMES, Dec. 23, 2010, at A30.

8. See Mansoura Ez-Eldin, *Date with a Revolution*, N.Y. TIMES, Jan. 21, 2011, at A19; Karim Fahim & Mona El-Naggar, *Across Egypt, Protests Direct Fury at Leader*, N.Y. TIMES, Jan. 26, 2011, at A1; Christine Hauser, *New Service Lets Voices from Egypt Be Heard*, N.Y. TIMES, Feb. 2, 2011, at A14; David D. Kirkpatrick, *Wired, Educated and Shrewd, Young*

almost all Internet access to the country.<sup>9</sup> Such efforts have not been limited to Egypt. In Burma and Tunisia, Iran and Libya, anti-government protestors have used the same technologies as Ravi to build support and momentum for their political movements.<sup>10</sup> Simultaneously, WikiLeaks founder Julian Assange has prompted an international diplomatic crisis by disclosing American diplomatic cables to international newspapers.<sup>11</sup>

Each of these cases, from Clementi and WikiLeaks, to the “It Gets Better Project” and the Middle Eastern and North African cases, reveals the power of the Internet in the modern age. In an era of ubiquitous cameras and mobile computers, social networks, blogs, and YouTube, individuals have an unprecedented power to publish information to the world. Much of this information is trivial and mundane. But as these examples suggest, the power to broadcast to the world has tremendous potential to be used for good and for evil, to help and to harm. The *Clementi* case illustrates the power of these technologies to invade privacy and harm, while the Egyptian example shows their power to unleash important political speech. Of course, there are difficult middle cases as well—what would happen if a newspaper were to post the Clementi video on its website? What happens when the news is also an invasion of privacy? As we navigate the contours of privacy and speech, law will inevitably play an important role. How should our law conceive of these privacy issues, and what tools should it use to approach them?

For better or worse, American law currently uses tools developed in the nineteenth and mid-twentieth centuries to deal with these problems of the twenty-first. For the past 120 years, discussions of privacy in American law have been dominated by the tort conception of privacy

*Egyptians Guide Revolt*, N.Y. TIMES, Feb. 10, 2011, at A1; David D. Kirkpatrick & Michael Slackman, *In New Role, Egypt Youths Drive Revolt*, N.Y. TIMES, Jan. 27, 2011, at A1; Jennifer Preston, *Movement Began with Outrage and a Facebook Page That Gave It an Outlet*, N.Y. TIMES, Feb. 6, 2011, at A10; Anthony Shadid, *Yearning for Respect, Arabs Find a Voice*, N.Y. TIMES, Jan. 30, 2011, at A10.

9. Noam Cohen, *Egyptians Were Unplugged, and Uncowed*, N.Y. TIMES, Feb. 21, 2011, at B3; James Glanz & John Markoff, *Egypt's Autocracy Found Internet's 'Off Switch*, N.Y. TIMES, Feb. 16, 2011, at A1; Matt Richtel, *Egypt Halts Most Internet and Cell Service, and Scale of Shutdown Surprises Experts*, N.Y. TIMES, Jan. 29, 2011, at A13.

10. Alan Cowell, *Protests Take Aim at Leader of Libya*, N.Y. TIMES, Feb. 17, 2011, at A14; Pheobe Kennedy, *Burma's Junta Can't Escape from the Net*, INDEP. (UK), Sept. 14, 2010, at 24; David D. Kirkpatrick, *Protests Spread to Tunisia's Capital, and a Curfew is Decreed*, N.Y. TIMES, Jan. 13, 2011, at A4; David D. Kirkpatrick & David E. Sanger, *A Tunisian-Egyptian Link That Shook Arab History*, N.Y. TIMES, Feb. 14, 2011, at A1; Brad Stone & Noam Cohen, *Social Networks Spread Iranian Defiance Online*, N.Y. TIMES, June 16, 2009, at A11.

11. Matthew Lee, *Leaked US Cables Reveal Sensitive Diplomacy*, REAL CLEAR POLITICS, Nov. 29, 2010, [http://www.realclearpolitics.com/news/ap/politics/2010/Nov/29/leaked\\_us\\_cables\\_reveal\\_sensitive\\_diplomacy.html](http://www.realclearpolitics.com/news/ap/politics/2010/Nov/29/leaked_us_cables_reveal_sensitive_diplomacy.html); Sarah Ellison, *Wikigate: The Twisted Inside Story of How Julian Assange Spilled the Government's Biggest Secrets*, VANITY FAIR, Feb. 2011, at 92.

advanced in 1890 by Samuel Warren and Louis Brandeis. In their famous article, “The Right to Privacy,” Warren and Brandeis argued that tort law should protect a person’s “inviolable personality” against their private affairs being “broadcast from the housetops,” by an increasingly intrusive press.<sup>12</sup>

Over fifty years later, William Prosser assessed the cases that had adopted the Warren and Brandeis theory, organized them into four categories, and used his influence as the leading torts scholar of his day to ensure that his scholarly pruning became recognized by the law.<sup>13</sup> Today, the law recognizes the same four privacy torts that Prosser announced in 1960: disclosure of private facts, appropriation of likeness, false light, and intrusion into seclusion.<sup>14</sup> These four torts share several elements, but the most important ones are those exemplified by the disclosure tort—publicity given to private facts that causes emotional harm.<sup>15</sup> Indeed, the disclosure tort conception of privacy is one that has been highly influential in American law, informing not just tort law, but civil and criminal statutes as well as widespread scholarly commentary.<sup>16</sup>

But at the same time, the disclosure tort has raised serious constitutional issues under the First Amendment, with many courts and scholars concluding that the disclosure tort is largely unconstitutional.<sup>17</sup>

12. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890); see also Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 128-31 (2007) [hereinafter Richards & Solove, *Privacy's Other Path*].

13. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); see also G. EDWARD WHITE, TORT LAW IN AMERICA: AN INTELLECTUAL HISTORY 176 (expanded ed. 2003); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1904-07 (2010) [hereinafter Richards & Solove, *Prosser's Privacy Law*].

14. RESTATEMENT (SECOND) OF TORTS §652A(2) (1977); Melville Nimmer, *The Rights of Privacy and Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954).

15. “One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” RESTATEMENT (SECOND) OF TORTS §652D (1977).

16. See 18 U.S.C. § 2511(1)(c) (2010) (providing criminal penalties when one “intentionally discloses . . . to any other person the contents of any wire, oral, or electronic communication” obtained through an ECPA violation); 18 U.S.C. § 2702(a)(1) (2010) (“[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.”); Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195 (1990); Harry Kalven, Jr., *Privacy in Tort Law – Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 330, 333-39 (1966); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983).

17. Jacqueline K. Rolfs, *The Florida Star v. B.J.F.: The Beginning of the End for the Tort of Public Disclosure*, 1990 WIS. L. REV. 1107, 1128 (1990); Edelman, *supra* note 16, at 1207; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); Zimmerman, *supra* note 16.

The conflict between privacy and speech is not merely an academic debate. Questions of information control and disclosure have become central to pressing questions of social policy in the digital age. How can we balance rights of privacy and rights of speech in the context of blogs, tweets, and other social networks?

This essay suggests a way forward. Part I outlines the theory and origins of tort privacy, paying particular attention to the common law tort of disclosure of private facts. Part II examines the conflict between disclosure privacy and free speech, concluding that because of the way American law has structured both free speech and the disclosure tort, the conflict is irreconcilable: We must ultimately choose between free speech or privacy protections along the lines of the disclosure tort. Part III demonstrates the limits of disclosure privacy in both traditional and social media contexts, arguing that the First Amendment should trump disclosure privacy in all but a narrow category of cases. But the harms the disclosure tort has tried but failed to remedy are real. The paper concludes by suggesting some ways other than disclosure privacy that the law can protect against some of these harms whilst also minimizing conflict with the First Amendment.

## I. THE ORIGINS AND THEORY OF TORT PRIVACY

The disclosure tort has become the most successful legacy of Warren and Brandeis's "The Right to Privacy." That article's central claim is that the common law should be read to recognize a tort protecting the emotions of individuals from disclosures of private information (whether by words or pictures) about their lives. The basic argument for disclosure privacy is thus the basic argument of the Warren and Brandeis article.

Although the precise origins of the Warren and Brandeis project are unclear, the evidence suggests that the original idea for the article came from Warren and not Brandeis.<sup>18</sup> Warren was a Boston Brahmin, a Harvard-educated lawyer and the heir to a successful family paper business.<sup>19</sup> He married Mabel Bayard, the daughter of Senator Thomas F. Bayard.<sup>20</sup> When the Warrens became the subject of unwanted

---

18. James H. Barron, *Warren and Brandeis, The Right to Privacy*, 4 *Harv. L. Rev.* 193 (1890); *Demystifying a Landmark Citation*, 13 *SUFFOLK U. L. REV.* 875, 891-907 (1979); Amy Gajda, *What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to the Right to Privacy*, 2008 *MICH. ST. L. REV.* 35, 44-57 (2008); Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 *VAND. L. REV.* 1295, 1302 (2010) [hereinafter Richards, *Brandeis*].

19. ALPHEUS THOMAS MASON, *BRANDEIS: A FREE MAN'S LIFE* 68 (1946); Barron, *supra* note 18, at 908-09.

20. MELVIN I. UROFSKY, *LOUIS D. BRANDEIS: A LIFE* 97 (2009); Gajda, *supra* note 18, at 36.

attention from the society pages of Boston newspapers, Warren enlisted Brandeis in the project, and the fruits of their labors were published in the Harvard Law Review in December 1890.<sup>21</sup> The result was an argument that the common law should protect a right to privacy. It was as brilliant as it was loose with existing Anglo-American precedent.<sup>22</sup>

I have written in greater detail about the Warren and Brandeis article elsewhere<sup>23</sup> and have no wish to duplicate those arguments here, but for present purposes three aspects of the article are relevant. First, the article sought to protect individuals against emotional harm—specifically the publication of private facts and photographs by journalists and others which produced hurt feelings. They argued that this “evil of the invasion of privacy” caused serious emotional and psychological damage.<sup>24</sup> “Instantaneous photographs and newspaper enterprise,” they argued, “have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”<sup>25</sup> The trade in gossip thus created by the press, the authors continued, included the publication of:

details of sexual relations and idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.<sup>26</sup>

Emotional harm was thus the very essence of the injury Warren and Brandeis were seeking to remedy.

Second, Warren and Brandeis targeted newspapers as the primary source of this injury, and the core defendant for their proposed tort. They argued that although personal gossip was harmful, widely-circulated gossip by journalists was vastly more dangerous, and caused “the lowering of social standards and of morality.”<sup>27</sup> The threat posed by newspapers trading in gossip was thus a threat not just to individual feelings, but also to social morality itself. Viewed in this way, even harmless gossip would

21. Richards, *Brandeis*, *supra* note 18, at 1302.

22. Richards & Solove, *Privacy's Other Path*, *supra* note 12, at 129-31.

23. *See id.*; Richards, *Brandeis*, *supra* note 18.

24. Warren & Brandeis, *supra* note 12, at 195.

25. *Id.*

26. *Id.* at 196.

27. *Id.*

have the effect of “inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance.”<sup>28</sup> By crowding out more serious and important information in the minds of citizens, gossip lowered social standards and encouraged “the weak side of human nature” to flourish.<sup>29</sup> Protecting privacy was thus essential to protect not just hurt feelings, but the level of public discourse itself. But by conceptualizing the tort in this way, “The Right to Privacy” called for liability of the press for disclosing truthful private information—a tort against true publications that hurt people’s feelings. By crafting the tort in such a way, “The Right to Privacy” gave birth to a tort that was inevitably going to come into conflict with the constitutional values protected by the First Amendment.

The third relevant dimension of “The Right to Privacy” was its reliance on the public/private distinction, both to the nature of “private” versus “public” facts, and to the scope of legitimate press inquiry as to those facts. The proposed tort would only protect facts “concern[ing] the private life, habits, acts, and relations of an individual,”<sup>30</sup> but would not “prohibit any publication of matter which is of public or general interest.”<sup>31</sup> Thus, the tort would not prohibit the publication of information with a “legitimate connection” with the fitness of a candidate for public office or any actions taken in the public sphere.<sup>32</sup> Acknowledging that this principle was more along the lines of a rough sketch, the authors conceded that they had not provided “a wholly accurate or exhaustive definition,” and left the contours of the distinction to the common law method of case-by-case adjudication.<sup>33</sup> But they insisted that the new tort’s lodestone should be the idea that “[s]ome things all men alike are entitled to keep from popular curiosity, whether in public life or not, while others are only private because the persons concerned have not assumed a position which makes their doings legitimate matters of public investigation.”<sup>34</sup>

If Warren and Brandeis gave tort privacy its name and guiding principles, William Prosser gave it form and brought it into the mainstream of American tort law.<sup>35</sup> Although few courts adopted or

---

28. *Id.*

29. *Id.*

30. *Id.* at 216.

31. *Id.* at 214.

32. *Id.* at 216.

33. *Id.*

34. *Id.*

35. For a more detailed examination of Prosser’s ambivalent influences on the development

recognized privacy in the early years after Warren and Brandeis published their article, by the time Prosser began to write about privacy there were several hundred such cases.<sup>36</sup> Over four decades from the 1940s until the 1970s, Prosser worked to give the privacy torts order and form.<sup>37</sup> His principal contribution was to argue that the cases adopting the Warren and Brandeis formulation represented not just one tort but “four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by a common name, but otherwise have nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, ‘to be let alone.’”<sup>38</sup> Prosser described his four torts as follows:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.<sup>39</sup>

These four torts were recognized by the courts and today are the foundation of modern tort privacy.<sup>40</sup>

But Prosser’s influence on tort privacy was mixed. While he gave the torts a stature they had previously lacked, by including them as recognized causes of action in his casebooks and treatises, Prosser also limited tort privacy’s ability to evolve.<sup>41</sup> Today the four privacy torts remain on the books much as Prosser left them at his death in 1972—intrusion, disclosure, false light, and appropriation. Nevertheless, most states recognize some or all of Prosser’s privacy torts. For example, in *Lake v. Wal-Mart Stores*, Minnesota became the 46th state to recognize some or all of privacy torts.<sup>42</sup> The case involved the misappropriation and circulation in the community of holiday snapshots depicting the two female plaintiffs, Lake and Weber, “naked in the shower together.”<sup>43</sup> Unlike in the *Clementi* case, the photograph was apparently taken

---

of tort privacy, *see generally* Richards & Solove, *Prosser’s Privacy Law*, *supra* note 13.

36. Prosser, *Privacy*, *supra* note 13, at 388.

37. Richards & Solove, *Prosser’s Privacy Law*, *supra* note 13, at 1895-1903.

38. Prosser, *Privacy*, *supra* note 13, at 389.

39. *Id.*

40. Richards & Solove, *Privacy’s Other Path*, *supra* note 12, at 1907-08.

41. *Id.*

42. *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998).

43. *Id.* at 232.

consensually by Weber's sister who had gone on holiday with them. The plaintiffs had the film developed at Wal-Mart, only to discover a note when they collected the prints that some photographs had not been developed due to their "nature."<sup>44</sup> Over the next few months the plaintiffs became aware that the nude photographs had in fact been developed and were circulating in the community along with hurtful speculation about the plaintiffs' sexualities. Feeling their privacy to have been invaded, the plaintiffs sued Wal-Mart. Invoking both the Warren and Brandeis article and Prosser's *Restatement* formulation, the Court held that

Today we join the majority of jurisdictions and recognize the tort of invasion of privacy. The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close. Here [plaintiffs allege] that a photograph of their nude bodies has been publicized. One's naked body is a very private part of one's person and generally known to others only by choice. This is a type of privacy interest worthy of protection. Therefore, without consideration of the merits of Lake and Weber's claims, we recognize the torts of intrusion upon seclusion, appropriation, and publication of private facts.<sup>45</sup>

Although liability in privacy cases appears to be rare, *Lake* illustrates how the four privacy torts remain alive, and that they also have an application beyond press defendants.

## II. DISCLOSURE AND THE FIRST AMENDMENT CRITIQUE

Although the disclosure tort has been adopted in most states and influenced a variety of other kinds of privacy protections, it has always remained under something of a cloud because of its inherent tension with the free speech protections of the First Amendment. The conflict between the disclosure tort and speech was first recognized by its creators. Warren and Brandeis hoped that the public/private distinction would sufficiently balance privacy rights against free speech. They also acknowledged that their proposed tort should apply only to written disclosures of private fact, and not "grant any redress for the invasion of privacy by oral publication in the absence of special damage."<sup>46</sup> The authors explained that "[t]he injury resulting from such oral communications would ordinarily be so trifling that the law might well,

---

44. *Id.* at 233.

45. *Id.* at 235.

46. Warren & Brandeis, *supra* note 12, at 217.

in the interest of free speech, disregard it altogether.”<sup>47</sup> This passage is interesting not only because it shows that even Warren and Brandeis were aware that their proposed tort raised free speech issues, but also because it illustrates that their primary concern was written communication by newspapers as mass media.

Prosser had even greater misgivings than Warren and Brandeis about the constitutionality of the privacy torts, especially disclosure and false light. He worried that tort privacy threatened to upset the carefully-crafted balances that tort law had established, and his codification of the privacy cases into his treatises and the Restatement (of which he was the principal reporter) reflected these concerns. In an influential 1960 article, he lamented the trajectory that was bringing the disclosure tort in particular into conflict with the First Amendment. In contrast to defamation law, which protected press defendants through doctrinal mechanisms like the retraction statutes, the truth defense, proof of special damages, the disclosure and false light torts in particular lacked any such limitations. Prosser was worried that liability in privacy cases could arise from the publication of non-defamatory truthful facts or even “laudatory fiction.”<sup>48</sup> Even worse, Prosser argued, was the likelihood that under open-ended tests like “‘ordinary sensibilities’ or the ‘mores’ of the community as to what is acceptable and proper, the courts, although cautiously and reluctantly, have accepted a power of censorship over what the public may be permitted to read, extending very much beyond that which they have always had under the law of defamation.”<sup>49</sup>

Today, the concept of disclosure privacy is most clearly embodied in Section 652D of the Restatement (Second) of Torts. That section provides that

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.<sup>50</sup>

Reorganizing this language slightly, we can think of the disclosure tort as having three basic elements: (1) publicity given to (2) private, non-newsworthy facts that are (3) highly offensive. Remarkably, *each* of these elements creates tension with the First Amendment. For example, the publicity requirement is usually interpreted to require “public communication.” As the official comment to this section of the

47. *Id.*

48. Prosser, *Privacy*, *supra* note 13, at 422.

49. *Id.* at 423.

50. RESTATEMENT (SECOND) OF TORTS §652D (1977).

Restatement makes clear, publicity “means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.”<sup>51</sup> Publicity can be oral, written, or electronic, but “any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity[.]”<sup>52</sup> Because the publicity requirement is crafted in this way, the disclosure tort targets mass communications such as newspapers—exactly the kinds of publications likely to raise First Amendment concerns. By contrast, publicity is not triggered by communicating private facts “to a single person or even to a small group of persons.”<sup>53</sup> Some cases have read publicity more narrowly, allowing particularly harmful facts made known in a workplace, for instance.<sup>54</sup> But these cases remain a clear minority.

But because mass publicity is one of its key elements, the disclosure tort targets those disclosures most likely to raise First Amendment concerns because they bear a close resemblance to a news broadcast.<sup>55</sup> At the same time, the focus on mass publicity diverts attention away from other uses of words that may be both more injurious and less threatening to the First Amendment. Robert Post notes, for example, that “[w]e often care more about what those within our ‘group’ think of us than we do about our reputation among the strangers who comprise the general public. Yet the publicity requirement, as defined by the Restatement, would impose sanctions for the disclosure of a husband’s marital infidelity to the general public, but not for its disclosure to his wife.”<sup>56</sup> Recall once more the streaming of the Clementi sex video, which though announced on Twitter, was apparently only viewed by a relatively small number of people. Under the traditional definition of publicity in the disclosure tort, the circulation of a video to a small group of people would not by itself be actionable without some likelihood that the video became “a communication that reaches, or is sure to reach, the public.”<sup>57</sup>

51. *Id.* at cmt. a.

52. *Id.*

53. *Id.*

54. *See, e.g.,* Miller v. Motorola, 560 N.E.2d 900 (Il. App. 1990); *see also* Beaumont v. Brown, 257 N.W.2d 522 (Mich. 1977); *see generally*, DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW, 116 (3d ed. 2006) (collecting cases).

55. Cf. Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758-59 (noting that private speech “is of less First Amendment concern”).

56. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 992 (1989); *see also*, Jonathan B. Mintz, *The Remains of Privacy’s Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 425, 438 (1996).

57. RESTATEMENT (SECOND) OF TORTS §652D (1977).

The focus on publicity thus increases the constitutional risk, without necessarily focusing liability on the most harmful kinds of disclosures.

The second problem with the disclosure tort is that it requires judges to divide the world of press publications into public and private, requiring them to protect the public and hold liable the private. The public/private distinction comes into play in two areas of the common-law tort—the requirement that the information be “private,” and the limitation that the disclosure of information is not of “legitimate concern to the public.” Although these are today formally separate elements in the tort, it makes sense to treat them together. As Warren and Brandeis themselves recognized, these elements are usually related—information which is truly private is not fit for public consumption and vice versa.<sup>58</sup> Yet the distinction between private information and information that is protected in the interest of public debate can be a difficult one, because information can be in both categories at once (think Bill Clinton’s extramarital affairs) or can lie in the extremely fuzzy area between the two concepts, which are themselves poorly defined.

More difficult than the definitional problem is a substantive one: The idea that courts should police what publications are of “legitimate concern to the public” and which are not raises a serious risk of censorship. Warren and Brandeis recognized that this was a potentially fuzzy distinction, but they had faith in the ability of courts to police the line in a fair, principled, and determinate way.<sup>59</sup> Warren and Brandeis were writing before the First World War, during a period in American jurisprudence when First Amendment protections were thinly protected. Brandeis himself later admitted that he had not “thought through” the issues of the First Amendment until he was forced to rule on a series of important prosecutions under federal and state espionage acts from 1919-1927,<sup>60</sup> and there is evidence to believe that he backed away from his nineteenth century confidence in the ability of courts to police legitimate and illegitimate speech when he was confronted as a judge with the problems of the twentieth century. For example, Brandeis dissented from the Court’s recognition of a common law right preventing news services from the reprinting “hot news” gathered by competitors in *International News Service v. Associated Press*.<sup>61</sup> Brandeis argued that the “free use of knowledge and of ideas” could be curtailed by the recognition of a quasi-property right in news reports.<sup>62</sup> In a departure from the faith he placed in the common law’s ability to regulate the press in “The Right

---

58. See *supra* notes 28-32 and accompanying text.

59. Richards, *Brandeis*, *supra* note 18, at 1308.

60. *Id.* at 1340-41.

61. 248 U.S. 215 (1918).

62. *Id.* at 263.

to Privacy,” Brandeis suggested that while the common law “possesses capacity for growth and has often satisfied new demands for justice by invoking analogies or by expanding a rule of a principle,” this approach was unwarranted in the factual context of the news business.<sup>63</sup> Although common law rules could prove useful for simple legal problems involving only private interests, “with the increasing complexity of society, the public interest tends to become omnipresent.”<sup>64</sup>

Subsequent disclosure cases bore out Brandeis’s suspicion that while the line between public and private is easy to understand in the abstract, in practice it is very hard to draw with any confidence or predictability. And as the twentieth century marched on, judges (especially Brandeis himself) came to link freedom of speech to democracy and to believe that questions as important as what constitutes a matter of public concern were not only becoming too difficult to leave to courts, but should as a normative matter be left to individual citizens to decide for themselves.<sup>65</sup> In a recent article, Samantha Barbas argues quite convincingly that in a series of mid-century disclosure tort cases, judges deciding tort actions were in reality thinking through the basic elements of free speech law, including broadening the notion of what was a legitimate matter of public concern. Surveying the mid-century disclosure tort cases, Barbas shows how in the disclosure tort cases, judges recognized a social

expansion of the definition of “the news” to encompass a wide variety of information, including private facts, and a reassessment of the significance of the news media to modern social life. We see the emergence of the concept of “the public’s right to know” about the world through the news media, and the ideas that the purpose of the news is not only to inform citizens about the complex workings of modern society but to generate public discourse. For the news media to achieve this function, there must be robust legal and constitutional protection for a free press, and news content must be as extensive as the public’s interests and concerns.<sup>66</sup>

From the mid-twentieth century to the present, the Supreme Court’s First Amendment case law has taken a similarly broad view of the “legitimate public concern” standard. In *Time v. Hill*, the court first addressed a claim that privacy liability against the media offended the First Amendment, holding that a false light claim against *Time* magazine

---

63. *Id.*

64. *Id.*

65. See generally MARK A. GRABER, *TRANSFORMING FREE SPEECH: THE AMBIGUOUS LEGACY OF CIVIL LIBERTARIANISM* (1991); DAVID M. RABBAN, *FREE SPEECH IN ITS FORGOTTEN YEARS, 1870-1920* (1997); WHITE, *supra* note 13.

66. Samantha Barbas, *The Death of the Public Disclosure Tort: A Historical Perspective*, 22 *YALE J. L. & HUM.* 171, 173 (2010).

required the plaintiffs to satisfy the stringent actual malice standard from *New York Times v. Sullivan*.<sup>67</sup> Even though the case had been brought by a previously unknown family who had been the victim of a celebrated hostage ordeal, the Court held that the First Amendment required broad deference to the press's determination of what was in the public interest. As Justice Brennan put it,

The guarantees for speech and press are not the preserve of political expression or comment upon public affairs, essential as those are to healthy government. One need only pick up any newspaper or magazine to comprehend the vast range of published matter which exposes persons to public view, both private citizens and public officials. Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press. Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.<sup>68</sup>

*Time v. Hill* represents a foundational and enduring commitment of the modern First Amendment—the idea that free speech is valuable because it helps to preserve an informed citizenry, and the state should not attempt to proscribe the fit subjects for public debate.<sup>69</sup> *Snyder v. Phelps*, the Court's most recent word on the intersection between tort liability for emotional injury and the First Amendment, also applied this standard, giving strong protection to even offensive and unrefined speech on matters “of interest to society at large.”<sup>70</sup> These ideas are also traceable back to Louis Brandeis, and represent the germination of his mature free speech jurisprudence which is directly at odds with many of the assumptions and arguments of “The Right to Privacy.”<sup>71</sup>

The mature Brandeis seems to have the better argument with respect to the direct separation of public from private by courts in privacy tort cases. My claim here is not that the public-private line is indefensible or always unworkable, but rather to suggest that as Brandeis predicted in *INS v. AP*, disclosure tort cases applying the test in practice have required courts to engage in a process that is, in the words of one scholar, an

---

67. *Time v. Hill*, 385 U.S. 374 (1967) (citing *New York Times v. Sullivan*, 376 U.S. 254 (1964)).

68. *Id.* at 385 (quoting *Thornhill v. Alabama*, 310 U.S. 88 (1940)).

69. See Barbas, *supra* note 66, at 214.

70. *Snyder v. Phelps*, 131 S. Ct. 1207, 1216 (2011).

71. Richards, *Brandeis*, *supra* note 18, at 1323-34.

“abstract, circular, and highly indeterminate question.”<sup>72</sup> Moreover, because that indeterminacy operates in an area of First Amendment sensitivity, it raises additional constitutional concerns. Giving a court the power to declare information “illegitimate” under a malleable standard is to give that court the power to censor expression that it (or a jury) dislikes, and is at odds with modern commitments to the freedom of expression.

The third problem with the notions of tort privacy rooted in nondisclosure is the nature of the injury that the tort protects. Although Warren and Brandeis spoke in terms of the dignity of individuals whose private matters were made public, the injury the tort sought to remedy was psychological, rooted in embarrassment causing harm to what they called a person’s “inviolable personality.”<sup>73</sup> This move was part of a trend in cases in the late nineteenth and early twentieth century to broaden the conception of tort harm beyond physical and property injuries to include psychological injury.<sup>74</sup> In this respect both privacy and the emotional distress torts shared many similarities, and Prosser was involved in the shaping of both categories of these torts into their modern forms.<sup>75</sup> But remedying the emotional harm caused by words also conflicts with First Amendment norms. A central tenet of modern First Amendment law is the idea that words causing hurt feelings, without more, cannot be punished by the state or made the subject of civil liability. Thus, in *Cantwell v. Connecticut*, the Court held that the playing in a Catholic neighborhood of a vitriolic record denouncing the Pope was protected by the First Amendment even though the it “aroused animosity.”<sup>76</sup> Although two years later the Court held in *Chaplinski v. New Hampshire* that the First Amendment did not protect “fighting words” on the theory that words that wound do not contribute to the processes of free speech, the category of fighting words has rarely been litigated and the Court has never upheld a subsequent conviction under the fighting words theory, even when presented with strikingly similar facts.<sup>77</sup>

The idea that valuable speech must be protected notwithstanding any emotional harm it causes has continued to be a major feature of

72. Strahilevitz, *supra* note 16, at 921.

73. Warren & Brandeis, *supra* note 12, at 195.

74. See DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 175-76 (2008).

75. WHITE, *supra* note 13, at 173; Richards & Solove, *Privacy's Other Path*, *supra* note 12, at 1908-09.

76. 310 U.S. 296, 311 (1940).

77. 315 U.S. 568 (1942); see, e.g., *Gooding v. Wilson*, 405 U.S. 518, 528 (1972) (striking down an almost identical fighting words statute to the one it upheld in *Chaplinski* under an overbreadth theory); *Terminiello v. City of Chicago*, 337 U.S. 1, 4 (1949) (noting that speech “may indeed best serve its high purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger,” and striking down a fighting words statute for overbreadth).

modern First Amendment law. In *New York Times v. Sullivan*, the Supreme Court announced what commentators have called the “central meaning” of the modern First Amendment<sup>78</sup>—that the First Amendment is principally a tool advancing democratic self-government through public debate in the press that is “uninhibited, robust, and wide-open,” and which frequently calls for “vehement, caustic, and sometimes unpleasantly sharp attacks” on public men and women and their role in society.<sup>79</sup> Consequently, at least when it constitutes protected speech, expression has been strongly privileged at the expense of even serious emotional harm. Although *Sullivan* was not a privacy case, dealing instead with the related cause of action of defamation, subsequent cases have made clear that the *Sullivan* privilege for speech over emotional harm applies in the privacy area as well. *Time v. Hill*, as noted above, extended the actual malice requirement to false light invasion of privacy claims against the press. And in *Gertz v. Welch* and *Firestone v. Time*, the Court noted that granting damages for speech alleged to have caused emotional harm risks punishment merely for unpopular opinion.<sup>80</sup> Other cases involving claims under the disclosure tort and similar legal theories have also been consistently rejected in favor of First Amendment deference, though the Court has been careful never to declare the disclosure tort unconstitutional in all of its potential applications.<sup>81</sup>

The most important case involving the clash between free speech and emotional harm is *Hustler v. Falwell*.<sup>82</sup> That case made the strongest statement yet that tort liability for words causing emotional harm is a direct threat to the free exchange of information and ideas. At least where public figures are the subject of the intentional infliction of emotional distress, the First Amendment protects even “outrageous”

78. Harry Kalven, Jr., *The New York Times Case: A Note on “The Central Meaning of the First Amendment,”* 1964 Sup. Ct. Rev. 191, 208.

79. 376 U.S. 254, 270 (1964).

80. *Firestone v. Time*, 424 U.S. 448, 475 n.3 (1976); *Gertz v. Welch*, 418 U.S. 323, 349 (1974).

81. *See, e.g.,* *Bartnicki v. Vopper*, 532 U.S. 514, 526–28 (2001) (holding that a radio station cannot be prohibited from publishing newsworthy information of public concern, even where such information had been illegally obtained by a third party); *Fla. Star v. B.J.F.*, 491 U.S. 524, 526 (1989) (holding that a state statute prohibiting the publication of the name of a rape victim was unconstitutional as applied to a newspaper that had obtained the name from a “publicly released police report”); *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97 (1979) (holding the First Amendment prohibits a state from punishing a newspaper for publishing the name of a juvenile murder suspect because the press lawfully obtained the information); *Okla. Publ’g Corp. v. Okla. County Dist. Court*, 430 U.S. 308 (1977) (holding the First Amendment prevents a state court from prohibiting the media from publishing the name of a juvenile in a proceeding that a reporter attended); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975) (holding the name of a rape victim obtained by the press from public records cannot be prevented from being published by statute or made the basis for liability under the nondisclosure tort).

82. 485 U.S. 46 (1988).

attempts to cause emotional harm through crude caricature. Part of the problem is a practical one—it is difficult to separate out worthless speech causing emotional harm from valuable expression. Considering the question, Chief Justice Rehnquist noted that “if it were possible by laying down a principled standard to separate the one from the other, public discourse would probably suffer little or no harm. But we doubt that there is any such standard, and we are quite sure that the pejorative description ‘outrageous’ does not supply one.”<sup>83</sup> Moreover, the indeterminacy of the legal standard created by the emotional harm/valuable speech binary creates risks of censorship. As the Court put it,

“Outrageousness” in the area of political and social discourse has an inherent subjectiveness about it which would allow a jury to impose liability on the basis of the jurors’ tastes or views, or perhaps on the basis of their dislike of a particular expression. An “outrageousness” standard thus runs afoul of our longstanding refusal to allow damages to be awarded because the speech in question may have an adverse emotional impact on the audience.<sup>84</sup>

When it comes to separating worthless emotional harassment from protected speech, the parallels to the public/private problem are striking, especially when applied to public figures or public matters.

The practical problem of separating the protected from the unprotected is hard enough for courts acting in good faith, but the indeterminate legal standard creates a second problem—the risk of overt or implicit censorship on the basis of viewpoint or dislike of the speaker. Thus, in the recent case of *Snyder v. Phelps*, the Supreme Court concluded that, at least for speech on a matter of public concern delivered in a public place, an outrageousness requirement is insufficient to protect free speech, as it still allows a jury to punish speech because of its viewpoint. When tort injury conflicts with free speech, the Court concluded, free speech must win because “in public debate we must tolerate insulting, and even outrageous speech in order to provide adequate ‘breathing space’ to the freedoms protected by the First Amendment.”<sup>85</sup>

These three problems inherent in the design of the disclosure tort—the media as a target, the public/private problem, and damages based on emotional harm—have rendered the disclosure tort a highly limited and constitutionally suspect remedy. This is particularly true in the very cases

---

83. *Id.* at 55.

84. *Id.*

85. *Snyder v. Phelps*, 131 S. Ct. 1207, 1219 (2011) (quoting *Boos v. Barry*, 485 U.S. 312, 322 (1988)).

which it was created to address—actions against the media for publishing private facts causing emotional harm. Perhaps ironically, disclosure-based theories of relief might be more applicable when the press is not involved, as in contexts like *Lake* and *Clementi*, because these cases do not involve public figures and thus seem to raise less of a First Amendment threat. The Internet has, however, blurred the distinction between public and private figures, and between the press and others.<sup>86</sup> If anything, this makes the good faith line-drawing exercises between press/non-press, public/private, and emotional harm/protected speech all the more difficult for courts to perform; it also increases the risk of bad faith or pretextual censorship under vague standards.

As a result, both because of the design of the tort and as a result of the evolution of the law, tort privacy remedies for disclosure against the press are largely unconstitutional under current law. And as a basis for protecting privacy, tort privacy is a very limited remedy. The history of the development of disclosure privacy and free speech over the twentieth century thus reveals that we must ultimately make a choice—either categorically or on a case-by-case basis—between disclosure privacy and freedom of speech.

### III. THE LIMITS OF DISCLOSURE

If we must choose between disclosure privacy and speech in most cases, what choice or choices should we make? In this Part, I argue that when disclosure privacy conflicts with free expression, we should choose free expression, subject to a few limited exceptions. Although this question has taken on new importance over the past decade, the question has engaged prominent scholars across several generations.<sup>87</sup> At the risk

---

86. David Lat's essay in this volume makes many of these arguments in detail. See David Lat & Zach Shemtob, *Public Figurehood in the Digital Age*, 9 J. ON TELECOMM. & HIGH TECH. L. 403 (2011); see also Melissa A. Troiano, Comment, *The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447 (2006); Anthony Ciolli, *Bloggers As Public Figures*, 16 B.U. PUB. INT. L.J. 255 (2007).

87. See, e.g., THOMAS I. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 556 (1970); DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION* (2008) [hereinafter SOLOVE, *FUTURE OF REPUTATION*]; Edward J. Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis's Tort Petty and Unconstitutional as Well?*, 46 TEX. L. REV. 611 (1968); Harry Kalven, Jr., *Privacy in Tort Law—Were Warren & Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195 (1990); Marc A. Franklin, *A Constitutional Problem in Privacy Protection: Legal Inhibitions on Reporting of Fact*, 16 STAN. L. REV. 107 (1963); Amy Gajda, *Judging Journalism: The Turn Toward Privacy and Judicial Regulation of the Press*, 97 CAL. L. REV. 1039 (2009); Ruth Gavison, *Too Early for a Requiem: Warren and Brandeis Were Right on Privacy vs. Free Speech*, 43 S.C. L. REV. 437 (1992); Paul Gewirtz, *Privacy and Speech*, 2001 SUP. CT. REV. 139 (2001); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957

of oversimplifying a fairly complex debate, scholars have coalesced around one of two positions.

On the one hand are the First Amendment critics of disclosure privacy. These scholars argue that the disclosure tort is unconstitutional, and should be jettisoned entirely in the interests of free speech. As early as 1967, Harry Kalven argued that “fascination with the great Brandeis trade mark, excitement over the law at a point of growth, and appreciation of privacy as a key value have combined to dull the normal critical sense of judges and commentators and have caused them not to see the pettiness of the tort they have sponsored.”<sup>88</sup> Fifteen years later, Diane Zimmerman went further and suggested that the disclosure tort was not only unworkable in practice, but “created a cause of action that, however formulated, cannot coexist with constitutional protections for freedom of speech and press.”<sup>89</sup> Most recently, Eugene Volokh argued that “the right to information privacy – my right to control your communication of personally identifiable information about me – is a right to have the government stop you from talking about me.”<sup>90</sup> Unlike Kalven and Zimmerman, who were writing solely about the disclosure tort, Volokh’s First Amendment claims extend to almost the entirety of information privacy law.<sup>91</sup>

On the other hand, privacy scholars typically claim that disclosure privacy serves important social interests, and that we should be able to strike a balance between privacy and speech, preserving control over injurious gossip while maintaining a robust commitment to speech of legitimate public interest. For example, Robert Post maintains that the disclosure tort serves a social purpose in the “maintenance of rules of civility” that protect human dignity, and that in the “various and inconsistent applications of the ‘legitimate public concern’ test, one can trace the wavering line between the insistent demands of public accountability and the expressive claims of communal life.”<sup>92</sup> Daniel Solove argues that the disclosure tort can be balanced with the First

---

(1989); Roscoe Pound, *The Fourteenth Amendment and the Right of Privacy*, 13 W. RES. L. REV. 34 (1961); William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005); Frederick Schauer, *Free Speech and the Social Construction of Privacy*, 68 SOC. RES. 221 (2001); Volokh, *supra* note 17.

88. Kalven, *supra* note 87, at 328.

89. Zimmerman, *supra* note 16, at 293.

90. Volokh, *supra* note 17, at 1050-51

91. *Id.*

92. Post, *supra* note 87, at 1007-08. Post goes on to assert that “Common law courts, like the rest of us are searching for ways to mediate between these two necessary and yet conflicting regimes. We can understand the public disclosure tort, then, as holding a flickering candle to what Max Weber called in 1918 the ‘fate of our times,’ which is of course the ‘rationalization and intellectualization, and above all, . . . the ‘disenchantment of the world.’” *Id.* at 1008.

Amendment, and can apply to “speech of private concern.” He argues that Brandeis “reconciled free speech and privacy with the newsworthiness test,”<sup>93</sup> and that the law should do a better job striking a “delicate balance” between speech and privacy in individual cases.

While my personal sympathies lie closer to the privacy advocates, I think on balance the First Amendment critics have the better of the argument with respect to the disclosure tort, at least most of the time. When the First Amendment critique applies in the disclosure context, it ought to triumph. Post is correct that, in its Gilded Age origins, and in its protection of emotional harm and propriety, disclosure privacy protects against egregious breaches of etiquette. Fundamentally, because of the way it is structured to remedy emotional injury, tort privacy runs into almost intractable problems when it restricts speech protected by the First Amendment, whether by the press or other speakers.<sup>94</sup> The problem with Post’s theory is that the core of the modern First Amendment protects a right to offend in furtherance of the robust exchange of ideas and information. First Amendment rights must trump disclosure privacy except in cases of truly extraordinary disclosures of private information. This is the case not merely as a formal matter because it applies the First Amendment rather than common law interests, but because free speech is a more important value.

But what about the sort of “delicate balance” that Solove calls for? As Part II demonstrated, the design of the common law disclosure tort renders it particularly subject to abuse by well-meaning courts as well as those who might use it as a pretext for censorship. In extraordinary cases, perhaps involving sexually-themed disclosures such as sex tapes, tort privacy might be able to survive a direct clash with the First Amendment. A few such cases impose liability for psychological injuries over free press challenges.<sup>95</sup> But such cases are likely to remain outliers, and appropriately so. As Brandeis himself grudgingly recognized later in life, a tort-based conception of privacy protecting against purely emotional harm must remain exceptional in a constitutional regime dedicated to speech, publicity, and disclosure.<sup>96</sup>

How, then, should courts balance free speech against privacy in practice? While the free speech critique of tort privacy should triumph where it applies, we should recognize that the First Amendment does not immunize all true statements by all speakers (or even all journalists).

93. SOLOVE, *FUTURE OF REPUTATION*, *supra* note 87, at 129, 160.

94. Zimmerman, *supra* note 16; Volokh, *supra* note 17.

95. *See, e.g., Michaels v. Internet Entm’t Grp., Inc.*, 5 F. Supp. 2d 823 (C.D. Cal. 1998) (granting a preliminary injunction barring the Internet distribution of a sex video made by celebrity couple plaintiffs, notwithstanding the defendant’s claims of newsworthiness).

96. Richards, *Brandeis*, *supra* note 18, at 1323-24.

Even though Warren and Brandeis's core case of disclosure of private embarrassing facts by the press is largely unconstitutional, it does not follow that all privacy claims (even against the press) are unconstitutional, too. Under current law, the well-established rule is that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order."<sup>97</sup> Unpacking this standard suggests four exceptions to the general principle that press publication of the truth is always constitutionally protected.

First, if the information disclosed is not true, all bets are off, and we return to defamation law, which remedies false statements of fact. Of course, American defamation law after *New York Times v. Sullivan* is quite press-friendly, but where the information is false and intentionally disclosed, the press can be held liable under the actual malice standard for public figure plaintiffs, or lower standards for private or limited-purpose public figures.<sup>98</sup>

If the information disclosed is not "lawfully obtained," the press can be held liable under a second theory. In *Bartnicki v. Vopper*, a radio DJ broadcast a recording of an intercepted telephone call that had been left in his mailbox by an unknown person. The Court held that even though the journalist knew the conversation had been illegally obtained in violation of the federal Wiretap Act, the First Amendment protected its broadcast.<sup>99</sup> But the Court also noted that if the journalist had participated or solicited the wiretap, the First Amendment would not protect him from civil or criminal punishment:

Our holding, of course, does not apply to punishing parties for obtaining the relevant information unlawfully. It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.<sup>100</sup>

This is consistent with the idea in First Amendment law that the press has no exemption from "generally-applicable laws"—that the press should have wide discretion in being able to disseminate ideas and

---

97. *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 102 (1979). The Supreme Court most recently reaffirmed this standard explicitly in *Bartnicki v. Vopper*, 532 U.S. 514 (2001).

98. *See, e.g.*, ERWIN CHEMERINSKY, CONSTITUTIONAL LAW (2000).

99. *Bartnicki*, 532 U.S. at 535.

100. *Id.* at n.19 (quoting *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972)).

information, but that this discretion does not allow exemptions from the ordinary tort, contract, property, and regulatory laws that govern all of us in our daily affairs without dictating the content of our expression.<sup>101</sup> From this perspective, there is a crucial distinction between breaking the law to obtain information (whether by wiretapping, trespassing, hacking, or other means) and the innocent dissemination of news generated by that law-breaking.<sup>102</sup> It also suggests, going beyond disclosure for a moment, that restrictions sounding in trespass or other theories protecting against the collection of embarrassing information are less problematic from a First Amendment perspective when they remedy harms flowing from the *collection* and not the *disclosure* of the private information.

A third exception under current law is that disclosures of private information that is not of legitimate concern to the public (or “newsworthy”) are entitled to a lower level of First Amendment protection. Solove relies on this exception when he argues that because the Supreme Court has hinted that speech on matters of private concern is less protected than other kinds of speech, the Court “has thus left open an area for the public-disclosure tort to thrive.”<sup>103</sup> This interpretation of the law probably overstates the vitality not only of the disclosure tort, but of disclosure-based theories of privacy more generally. The Supreme Court in particular has been quite reluctant to second-guess the editorial judgments of journalists. For instance, in *Bartnicki* the Court deferred quite readily to the media’s argument that the intercepted telephone conversation was newsworthy.<sup>104</sup> Most courts tend to define what is newsworthy by what is published by the press, under the theory that the press is the best judge of what sells papers, but certain kinds of outrageous disclosures have been held to lie beyond the pale. In such extraordinary cases, usually involving sexually-themed disclosures, tort privacy can survive a direct clash with the First Amendment protections given to the press. As discussed earlier, a few such cases impose liability for psychological injuries over free press challenges, most famously one granting an injunction to actress Pamela Anderson against the distribution of a graphic sex tape.<sup>105</sup> But as noted above, such cases must

---

101. See, e.g., *Cohen v. Cowles Media*, 501 U.S. 663 (1991) (holding journalist liable for breach of promise of confidentiality to a source over First Amendment objections).

102. See Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650 (2009).

103. SOLOVE, *FUTURE OF REPUTATION*, *supra* note 87, at 129.

104. *Bartnicki*, 532 U.S. 514.

105. See, e.g., *Michaels v. Internet Entm’t Grp., Inc.*, 5 F. Supp. 2d 823 (C.D. Cal. 1998) (granting a preliminary injunction barring the Internet distribution of a sex video made by celebrity couple plaintiffs, notwithstanding the defendant’s claims of newsworthiness). See *supra* note 95 and accompanying text.

remain outliers. Insofar as the public disclosure tort remedies Post's breaches of etiquette, it is only the most psychologically harmful and outrageous breaches of social norms that would seem to satisfy this exception.

More generally, however, courts are reluctant to second-guess the views of individual citizens about what the legitimate topics of public debate really are. The power to declare facts or topics to be off limits to public discussion is in a very real sense the power to censor, and modern First Amendment theory is built around this idea—traceable to Justice Brandeis' opinion in *Whitney v. California* that the normal remedy for harmful, dangerous, or otherwise “bad” speech is more speech rather than censorship.<sup>106</sup> Given that courts have routinely held that the publication of the name of a rape victim is “newsworthy,”<sup>107</sup> and particularly given censorship concerns in this area, it is hard to imagine a category beyond the dissemination of videos of sexual or other intimate bodily activities that would satisfy this exception.

The fourth and perhaps largest exception to the principle of protection for true facts is the presence of a state “interest of the highest order.”<sup>108</sup> Restrictions on the publication of true, newsworthy, lawfully obtained facts invoke strict scrutiny, but one could imagine interests that could survive a strict scrutiny challenge. For instance, national security could trump the First Amendment if a newspaper is disclosing the lawfully-obtained names of spies, or (to use an old trope that runs through the case law) the “publication of the sailing date of transports or the number and location of troops” or other time-sensitive military secrets.<sup>109</sup> In the “Pentagon Papers” case of *New York Times v. United States*, the Court held that publication of the Pentagon Papers could not be enjoined absent a showing of a more serious threat to national security than the Nixon Administration made. The case stands for the proposition that it can be hard to get an injunction *before* publication because of prior restraint concerns, but it says nothing authoritative about whether the press can be punished *after* publication for injuring national security.<sup>110</sup> Under current law, for example, it is a federal crime for anyone to disclose defense secrets that could be used to the “detriment of the United States or to the advantage of any foreign nation.”<sup>111</sup> This statute is likely constitutional even as applied to the disclosure of true, newsworthy, lawfully-obtained facts, but only as

106. *Whitney v. Cal.*, 274 U.S. 357, 376 (1927) (Brandeis, J., dissenting).

107. *E.g.*, *Fla. Star v. B.J.F.*, 491 U.S. 524, 526 (1989).

108. *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 103 (1979).

109. *E.g.*, *New York Times v. United States*, 403 U.S. 713, 726 (1971) (Brennan, J., concurring) (quoting *Near v. Minn.*, 283 U.S. 697, 716 (1931)).

110. In this regard, see Justice White's concurrence, *Id.* at 730-40 (White, J., concurring).

111. 18 U.S.C. § 793(e).

applied to materials for which the government can prove an actual and serious threat to national security.

The problem with the “interest of the highest order” exception for the constitutionality of disclosure privacy is that the showing necessary to satisfy the exception is extremely high—the compelling government interest and least-restrictive means required to satisfy First Amendment strict scrutiny. It is no coincidence that the standard example given here is harm to national security caused by the disclosure of defense secrets or dangerous technical information like the construction of bombs or weapons of mass destruction. In such cases the potential harm is lots of dead soldiers.

By contrast, it is unlikely that disclosure privacy could qualify as a sufficiently compelling interest except in the most extraordinary of cases. For example, in a line of free speech cases seeking the withholding of true but harmful information, very few interests other than national security have survived the scrutiny that this exception requires. In the *Landmark Press* case, the Court held that the confidentiality of a state judicial ethics investigation was an insufficiently strong interest to punish the press from divulging lawfully obtained information about an ongoing procedure.<sup>112</sup> Central to the Court’s reasoning was the availability of a less restrictive means—rather than punishing the press for publishing the truth, it suggested, the state should first try the more modest step of taking steps to reduce the likelihood of leaks from state employees to the press.<sup>113</sup> In *Nebraska Press v. Stuart*, the state interest arrayed against the freedom of the press was of a constitutional magnitude—the fair trial rights of an accused defendant in a high-profile murder case whom the trial court sought to protect by enjoining reportage on his alleged confession.<sup>114</sup> The constitutional criminal procedure rights of the defendant would seem to be at least as strong as tort privacy rights.<sup>115</sup> But in this case as well, the Court held for the newspaper, reasoning that before taking the blunt step of restricting the free flow of true information in the press, the state could take other measures less restrictive of First Amendment rights, such as a change of venue, postponement of the trial until the media frenzy had abated, jury instructions to disregard facts learned outside the trial, or even sequestration of the jury.<sup>116</sup> The recent WikiLeaks dispute garnered much speculation about whether Assange could be punished for the

---

112. *Landmark Commc’ns v. Va.*, 435 U.S. 829 (1978).

113. *Id.*

114. 427 U.S. 539 (1976).

115. The leading English privacy law scholar Gavin Phillipson has made this point recently. See Gavin J. Phillipson, *Trial By Media: The Betrayal of the First Amendment’s Purpose*, 71 *L. & Contemp. Probs.* 15, 16-17 (2008).

116. *Id.*

disclosure of diplomatic cables under this exception, and experts were divided about whether even this disclosure could be punished without additional factors present such as hacking or solicitation of leaks.<sup>117</sup> Facing such a standard, the “state interest of the highest order” exception would also be a poor fit for all but the most egregious disclosure tort cases.

Let us return then to the example with which this essay began—whether disclosure tort theory would permit the punishment of something like the alleged sex video broadcast in *Clementi*. The punishment of someone who, like Ravi, was alleged to have secretly recorded a sex act would seem to be a relatively straightforward case under my interpretation of the First Amendment. Most clearly, the act of secret recording would be unlawful under the federal Video Voyeurism Prevention Act of 2004,<sup>118</sup> or other state tort doctrines including the privacy tort of intrusion into seclusion. Because the video was not lawfully obtained, the punishment of such a defendant would be unlikely to offend the First Amendment. In addition, because the facts of such a case are an outrageous breach of social norms, and it is hard to see any legitimate public concern in the secret sex tape of another, it could also be argued that this would be one of the rare cases that lacked any newsworthiness. But even though the First Amendment might not preclude liability, it would be unclear that facts like these would satisfy the common law disclosure tort. As noted earlier, the disclosure tort requires “publicity,” and if the covert sex tape were only shown to a small number of people, with no likelihood that the video would come to circulate in the community, this would not satisfy the publicity requirement in most jurisdictions.

What if a newspaper received a copy of the Clementi video and decided to host a copy on its website—could the press be held liable for violating the disclosure tort? If *Bartnicki* is any guide, the answer would appear to be “no.” Because the press did not participate in the secret recording, the information would have been lawfully obtained by the press. Moreover, it is much harder in the case of press publication to argue that the tape would not now be “of legitimate concern to the public.”<sup>119</sup> When a video like Clementi’s sparks a public debate on cyber-bullying and acceptance of different sexual orientations, what was an easier case of non-newsworthiness for a non-press defendant becomes much more complicated because the video would then be at the center of a public debate. And when the debate centers around the contents of the

---

117. Nick Bravin, *See You in Court Mr. Assange*, SLATE (Dec. 10, 2010) <http://www.slate.com/id/2276592>.

118. 18 U.S.C. § 1801.

119. RESTATEMENT (SECOND) OF TORTS §652D (1977).

video, it becomes impossible to say that those contents are not of legitimate public concern. In this case, then, the nature of the disclosure tort could preclude liability even in a case of enormous emotional injury and widespread publication. And the result that the disclosure tort could fail to protect even its core case shows the limits of disclosure as a theory of liability.

## CONCLUSION: RETHINKING INVASION OF PRIVACY

Think back to why, in the last example, punishment of the secret recorder of a sex tape was relatively unproblematic: Because the recorder had broken the law by recording the tape, punishment for its disclosure was less troubling from a First Amendment perspective because it punished the act of recording and not any act of speaking or disclosure. But if secret recorders can be punished for their surveillance, why bother with punishing the subsequent disclosure at all, particularly if invoking a disclosure theory creates additional doctrinal problems, both in terms of the structure of the tort and its complicated relationship to the First Amendment? One answer is that disclosure allows punishment and deterrence of downstream viewers—those like the press who have otherwise lawfully obtained the recording and who view or disclose it themselves. But we saw in both the example and the *Bartnicki* case that downstream users can invoke First Amendment protections not available to the secret recorder.

Recall also from the example, that the secret recorder had violated the common law tort of intrusion against seclusion. That tort provides that

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.<sup>120</sup>

All of the elements of intrusion are satisfied by the example as well—we have (1) an intrusion (the secret recording) into (2) seclusion or private affairs (having sex in one's bedroom) that is (3) highly offensive (most people would be outraged to find secret listeners or hidden cameras in their bedrooms). However, there is an important difference between intrusion and disclosure—unlike disclosure, which requires the act of disclosure of words or images, no act of expression is necessary to satisfy the intrusion tort. Publication is only relevant to intrusion when damages are computed. Thus, unless we are prepared to recognize a First

---

120. *Id.* at § 652B.

Amendment right to break laws in pursuit of gathering news<sup>121</sup> or to take secret video,<sup>122</sup> the intrusion tort has been satisfied without implicating the First Amendment at all.

The intrusion tort shares more with the disclosure tort than a common origin in the Warren, Brandeis, and Prosser traditions. It shares both the element of private information and the element of high offensiveness to a reasonable person, making it another illustration of Post's argument that the privacy torts are best understood as remedies for gross breaches of social etiquette. But disclosure and intrusion are different breaches of good manners—whereas disclosure protects against emotionally harmful gossip, intrusion often protects against emotionally harmful collection of the gossip, by a secret recorder, secret listener, or other intruder.<sup>123</sup> Because the elements of the tort do not create civil liability for speech, thereby directly affecting the scope of public debate, the intrusion tort does not implicate heightened First Amendment concerns.<sup>124</sup> Moreover, if we are interested in protecting against what we colloquially call “invasions of privacy,” the intrusion model is a better fit with our intuitive linguistic understandings of that metaphor. Secret cameras would seem to “intrude” on our privacy more directly than publications about us that hurt our feelings. Thus, as we structure legal protections to protect private information from disclosure, the law should focus on preventing unwanted collections or accumulations of information, rather than preventing the dissemination of already-collected information.

Going beyond intrusion, there are other ways to remedy privacy harms that create fewer constitutional problems than the disclosure tort. We have become accustomed to thinking about privacy in terms of Prosser's four torts, but there are other torts sharing elements with some or all of the privacy torts that can also be used to regulate information. For example, there is a close analogy between intrusion and trespass, with the primary difference being that intrusion protects emotional harm from invasions into private areas or relationships, while trespass protects property rights from similar invasions. But trespass is in reality a kind of

121. *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505(4th Cir. 1999); *Desnick v. Am. Broad. Cos., Inc.*, 44 F.3d 1345 (7th Cir. 1995); *Dietemann v. Time*, 449 F.2d 245 (9th Cir. 1971); Rodney A Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW U. L. REV. 1099 (2002).

122. In a recent article, Seth Kreimer makes a creative argument to this effect. Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PENN. L. REV. 335 (2011).

123. This is the fact pattern of the famous intrusion case of *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964), in which a landlord had installed a secret listening device in the bedroom of his tenants, a married couple. But intrusion can also remedy invasions of private spaces that do not collect information—for example, a pattern of harassing phone calls that invade the tranquility of a victim's home.

124. See Solove & Richards, *supra* note 102.

privacy tort as well—protecting the privacy of the home from invasion, and another tort that creates fewer First Amendment problems than disclosure.

Breach of confidence is another privacy tort that has been underappreciated as a tool to regulate disclosures of embarrassing or harmful information.<sup>125</sup> Recall that in the press privacy cases, a less restrictive means than punishing disclosure was to prevent the press from collecting the information in the first place, rather than allowing the state to directly censor the speech under a disclosure theory. The press (or others) can obtain information by trespassing or intruding into private areas, or it can obtain it through a leak. Both the breach of confidence tort or confidentiality rules more generally allow the regulation of disclosure in a way that is less troubling from a First Amendment perspective than the disclosure tort. This is the case because confidentiality remedies not the emotional injury of published words, but instead the breach of an assumed duty.<sup>126</sup> Confidentiality has limits, too; most notably, it typically applies only to duties that are voluntarily assumed. But unlike the limits of disclosure, the limits of confidentiality enhance its consistency with our First Amendment commitments to robust public debate.<sup>127</sup>

The issues of press and privacy raised by the rise of social networks, incidents like the Clementi suicide and WikiLeaks are likely to become some of the most important and difficult facing our society in the Information Age. Of course, law will not provide all the answers, but it must provide some answers, if only to regulate the competing demands of publicity and non-disclosure that these cases raise. Law will be necessary to determine whether a case is more like Ravi's tweeting in the Clementi suicide, or more like the tweets of the democracy protesters in Cairo's Taksim Square. At the same time, it is important to realize that the harms from privacy are real. Just because the disclosure tort is largely unconstitutional, it does not mean that many of the psychological injuries it seeks to remedy are not substantial. A broader and more imaginative conception of tort privacy can hopefully help us to protect against some of those harms, either through tort law or other forms of law modeled on tort, and also to avoid the conflict with First Amendment values that the disclosure model produces.

---

125. Richards & Solove, *Privacy's Other Path*, *supra* note 12, at 123.

126. See Solove & Richards, *supra* note 102.

127. *Id.*

# THE VALUE OF DETECTIVE STORIES

AMY GAJDA\*

|      |   |     |
|------|---|-----|
| I.   | A HISTORY OF DETECTIVE STORIES AND LAW.....   | 386 |
| II.  | A PROSECUTOR’S FALL AND A MODEL’S MURDER: NEWS<br>OR PUNISHABLE SENSATIONALISM? ..... | 391 |
| III. | A CHILL IN REPORTING CRIME NEWS .....   | 399 |
|      | CONCLUSION.....   | 401 |

On a recent Sunday morning, *The Times-Picayune*, a newspaper from New Orleans, carried news that two young people had been arrested for an arson death, that a jury had convicted a man of killing a waitress in a robbery, and that a 15-year-old escapee from a youth detention facility had been recaptured. Those three stories were among the six main stories making up the first two pages of the local section of the newspaper.<sup>1</sup>

That same day, the main website pages of *The New York Times*, *The Washington Post*, and the *Chicago Tribune* featured similar police-related coverage. In New York, the *Times* reported that a suspect in a weekend murder spree had been arrested.<sup>2</sup> In Washington, D.C., a highly-placed story focused on the sentencing hearing for the man convicted in the murder of Chandra Levy, a congressional intern murdered by someone who had kidnapped her while she was jogging ten years earlier.<sup>3</sup> And in Chicago, all six “breaking news” stories on the *Tribune’s* website had some connection with a police investigation: charges in a double homicide, charges in a girl’s death, an arrest for animal neglect, a missing girl found, a death in a parking garage, and a house fire.<sup>4</sup>

---

\* Associate Professor of Law, Tulane University Law School.

1. Kari Dequine, *Two Booked in Woman’s Death*, TIMES-PICAYUNE, Feb. 13, 2011, at B1 (Metro Edition); *Jury Finds Man Guilty of Second-Degree Murder*, TIMES-PICAYUNE, Feb. 13, 2011, at B2; *Youth Escapee Apprehended*, TIMES-PICAYUNE, Feb. 13, 2011, at B2.

2. Robert D. McFadden & Al Baker, *Suspect in Brooklyn Stabbing Rampage is Captured*, N.Y. TIMES (Feb. 12, 2011), [http://www.nytimes.com/2011/02/13/nyregion/13stab.html?\\_r=1&chp](http://www.nytimes.com/2011/02/13/nyregion/13stab.html?_r=1&chp).

3. Keith L. Alexander, *Guandique Sentenced to 60 Years for Levy Murder*, WASH. POST (Feb. 12, 2011), <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/11/AR2011021103591.html?hpid=topnews>.

4. *Chicago Breaking News*, CHI. TRIB., <http://www.chicagotribune.com> (last visited Feb. 13, 2011, 7:20 AM).

If there is one type of news that is routinely covered in media, it is what I am calling here “detective stories”: news items that report the details of a crime or a criminal investigation or an arrest or a trial or a sentencing. For those living near the scene of the crime or some other police activity, the stories offer an important alert to neighborhood trouble, update residents as the investigation moves forward, and offer them some comfort when a perpetrator is eventually caught. The stories detail human relationships gone terribly wrong, drug dangers, and an inexplicable disregard for humanity. They also often detail bold courage. *The New York Times*’ story on the murder spree arrest, for example, outlined investigating officers’ fearless moves to apprehend the suspect in a subway train after a worried witness spotted the fugitive onboard. Even though *The New York Times* has a decidedly national readership, the story of the subway arrest was the eighth most-viewed by readers that Sunday morning,<sup>5</sup> indicating great public interest in a story that directly affected only a few.

And yet recent decisions by a handful of courts seem to hint at a limit to such coverage. These courts have punished media for reporting the arrest of a prosecutor, for publishing nude photos of a murder victim, and for reporting on somewhat mundane criminal matters.<sup>6</sup> In many of the decisions, the courts criticize media both soundly and broadly, with great implications both for future cases and for editorial decisions on news coverage. This symposium piece offers a historical perspective on detective stories, it explores recent cases that seem to push some detective stories back to a time when patrician attitudes quashed similar coverage, and it warns ultimately that courts deciding such cases need to recognize that they have a marked and potentially unconstitutional chilling effect on press freedoms.

## I. A HISTORY OF DETECTIVE STORIES AND LAW

In 1890 Samuel D. Warren and Louis Brandeis wrote *The Right to Privacy*<sup>7</sup> and, though it took decades, ultimately changed privacy law as we know it. Their message was a simple one: all persons deserved the right to be let alone and an out-of-control media threatened that sanctuary. The two authors criticized news reporting that they argued had invaded domestic tranquility,<sup>8</sup> lowered social standards and

---

5. *Most Popular*, N.Y. TIMES, <http://www.nytimes.com/gst/mostpopular.html?src=hp1-0-M> (last visited Feb. 13, 2011 7:30 AM).

6. *See, e.g.*, *Conrad v. NBC Universal, Inc.*, 536 F. Supp. 2d 380 (S.D.N.Y. 2008); *Toffoloni v. LFP Publ’g Grp., LLC*, 572 F.3d 1201, 1204 (11th Cir. 2009).

7. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

8. *Id.* at 195.

morality,<sup>9</sup> and threatened to crush enthusiasm for the robustness of life.<sup>10</sup>

But in spite of this railing against the news media of the day, even Warren and Brandeis recognized the value in a different sort of newspaper reporting. The right to privacy, the two authors wrote, “does not prohibit any publication of matter which is of public or general interest.”<sup>11</sup> They seemed to suggest that persons of their own stature, intellect, and station in life should decide what should become news, suggesting that “personal gossip” of great interest to the uneducated masses had lowered social standards and morality.<sup>12</sup> Their guidance would assist those “ignorant” and “thoughtless” who hungered for gossip, unwitting victims of the newspaper enterprise.<sup>13</sup> But even cultured would-be editors like Warren and Brandeis recognized the news value in stories in the public interest, those involving people who have, in some way, “renounced the right to live their lives screened from public observation.”<sup>14</sup>

William Prosser attempted to categorize existing privacy cases in a law review article that came 70 years later, *Privacy*.<sup>15</sup> Prosser developed a more explicit exception for stories involving crime, suggesting strongly that those who reported on criminal activity and the resulting investigation should never be liable for what they had published. News, he explained without equivocation, includes homicides and other crimes, arrests, public raids, suicides, accidents, and police reports.<sup>16</sup> He suggested that “the accused criminal” who, of course, would assiduously try to avoid publicity and would strongly desire privacy after his wrongdoing should not have his wishes fulfilled. Publishers could, in Prosser’s mind, satisfy the public’s obvious and understandable curiosity about their villains and victims and still stay comfortably within the bounds of law.<sup>17</sup>

The Second Restatement of Torts, greatly influenced by Prosser, contains similar sentiments but goes even further. Publicity Given to Private Life<sup>18</sup>—one of the four privacy torts outlined in the Restatement—defines explicitly those stories Warren and Brandeis suggested would be in the legitimate public interest. These would include crime stories, even those that report the names of rape victims.

---

9. *Id.* at 196.

10. *Id.*

11. *Id.* at 214.

12. *See id.*

13. *See id.* at 196, 214.

14. *Id.* at 214.

15. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

16. *Id.* at 412.

17. *Id.* at 413-14 (listing as examples multiple cases involving crime stories).

18. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

Crime's unfortunate victims, the Restatement authors explain, have sadly become part of a news event and, therefore, have properly become persons of public interest and an important part of a news story.<sup>19</sup> "[P]ublishers," the authors wrote, "are permitted to satisfy the curiosity of the public as to its . . . victims[ ] and those who are closely associated with them."<sup>20</sup>

But the Restatement saves the greatest wave of available news coverage for those persons police believe are responsible for criminal activity: "Those who commit crime or are accused of it may not only not seek publicity but may make every possible effort to avoid it," the Restatement notes, echoing Prosser in *Privacy*, "but they are nevertheless persons of public interest, concerning whom the public is entitled to be informed."<sup>21</sup>

The illustrations used in the Restatement help show the depth of possible news coverage relating to crime, with many examples based on actual cases decided by courts: murder coverage that includes a suspect later acquitted whose "past history and daily life" is explored in news accounts;<sup>22</sup> a photograph of a woman whose husband is murdered;<sup>23</sup> a police raid and resulting coverage of an unconnected customer;<sup>24</sup> a man on trial for sedition who, it is reported, works where he can overhear key government conversations;<sup>25</sup> and reports of an illegal street race with an accompanying photo of a driver's father who refused to be interviewed.<sup>26</sup> Admittedly, the Restatement suggests that some former criminals who have been rehabilitated over many years may have a cause of action against journalists who report their criminal past, but the Restatement authors purposefully make such liability conditional and, therefore, not certain.<sup>27</sup>

Finally, the Restatement adds additional detective stories to the category of acceptable news, broadening Prosser's list to include "publications concerning homicide and other crimes, arrests, police raids, suicides, . . . accidents, fires, . . . a death from the use of narcotics," police reports, "and many other similar matters of genuine, even if more or less deplorable, popular appeal."<sup>28</sup>

The clear message from the Restatement, commonly accepted by

---

19. *Id.* cmt. f.

20. *Id.*

21. *Id.*

22. *Id.* cmt. f, illus. 13.

23. *Id.* cmt. f, illus. 16.

24. *Id.* cmt. f, illus. 17.

25. *Id.* cmt. h, illus. 18.

26. *Id.* cmt. i, illus. 21.

27. *Id.* cmt. k, illus. 26.

28. *Id.* cmt. g.

courts in privacy cases across the nation, is that crime news, even crime news that is reported robustly, is protected under the First Amendment for its news value.

But the rich history of protection for detective stories goes beyond mere scholarly definition. Interestingly, in both 1931 and again in 1948, the United States Supreme Court decided cases involving detective stories and drafted opinions very much in line with the reasoning put forth by Warren and Brandeis and, later, Prosser. Both cases found unconstitutional statutes that made the selling of salacious detective stories against the law.

*Near v. Minnesota*<sup>29</sup> was the first of these cases. The Minnesota statute at issue made it a public nuisance to sell any “malicious, scandalous and defamatory newspaper, magazine or other periodical.”<sup>30</sup> As in *The Right to Privacy*, the authors of the statute wished to help promote the public welfare and to stop physical assaults at the angry hands of those featured in sleazy, push-the-envelope detective publications; the statute condemned scandalous reporting as “detrimental to public morals and to the general welfare”<sup>31</sup> and aimed to better society by ridding it of scandal sheets.

The publication at issue—*The Saturday Press*—had published a story about a Minneapolis Jewish “gangster” and how law enforcement officials apparently allowed his criminal deeds to continue. The article, quoted at length by the dissent, was decidedly anti-Semitic and admittedly disgusting at times. Such an article would necessarily violate the statute because it “circulate[d] charges of reprehensible [criminal] conduct,”<sup>32</sup> be they true or false.

But the Supreme Court found the statute a violation of the constitutional right to a free press. While the case was very much focused on the constitutionality of a preliminary injunction, the Court quoted the Continental Congress more generally and lauded the press and its importance in reporting wrongdoing, especially the wrongdoing of government leaders: “The importance of this [reporting] consists, besides the advancement of truth, science, morality, and arts in general, in its diffusion of liberal sentiments . . . whereby oppressive officers are shamed or intimidated, into more honourable [sic] and just modes of conducting affairs.”<sup>33</sup> Though the statute had a commendable purpose, the Court decided it would not fit within the confines of the Constitution.

29. *Near v. Minnesota*, 283 U.S. 697 (1931).

30. *Id.* at 701-02 (quoting 1927 Minn. Stat. 10123-1 to 10123-3 (Mason’s)).

31. *Id.* at 709 (quoting *State ex rel. Olson v. Guilford*, 174 Minn. 457, 461-62 (1928)).

32. *Id.* at 710.

33. *Id.* at 717 (quoting I JOURNAL OF THE CONTINENTAL CONGRESS, 1774-1789 104, 108 (1904)).

*Winters v. New York*<sup>34</sup> came seventeen years later. There, a similar statute made it a crime to publish anything “principally made up of criminal news, police reports, or accounts of criminal deeds, or pictures, or stories of deeds of bloodshed, lust or crime[.]”<sup>35</sup> Lawmakers had hoped that such a prohibition would protect minors from the exciting “criminal news and stories of bloodshed, lust or crime.”<sup>36</sup>

Here, the publication at issue was titled more sensationally: *Headquarters Detective, True Cases from the Police Blotter, June 1940*<sup>37</sup> and, as an earlier appeals court explained, “[t]he stories [were] embellished with pictures of fiendish and gruesome crimes, and [were] besprinkled with lurid [p]hotographs of victims and perpetrators.”<sup>38</sup> Headlined articles included the decidedly sensational *Bargains in Bodies, Girl Slave to a Love Cult*, and *Girls’ Reformatory*.<sup>39</sup> The appeals court had found the statute constitutional because it protected community morals through the paternalistically guiding editorial hand of the legislature.<sup>40</sup>

But here again the Supreme Court upheld the right of the magazine to publish the crime news it wanted to publish. “Though we can see nothing of any possible value to society in these magazines,” the Court wrote, “they are as much entitled to the protection of free speech as the best of literature.”<sup>41</sup> The statute, it found, was unconstitutional.

The Court later would later affirm protection for detective stories in a series of cases involving more traditional crime coverage. In *Time v. Hill*, where the plaintiffs’ claim arose from an article that sensationalized a home invasion and kidnapping, the justices wrote that they had “no doubt” that such coverage was “a matter of public interest[.]”<sup>42</sup> even though the article focused on a reenactment of the crime and not the crime itself. A little more than a decade later, in *Smith v. Daily Mail Publishing Company*,<sup>43</sup> the Court rejected a claim brought against a newspaper that had published a juvenile offender’s name as part of crime coverage. And a few years after that, the Court protected even more explicit news coverage of a rape, holding that it “involved a matter of paramount public import: the commission, and investigation, of a violent crime which had been reported to authorities.”<sup>44</sup>

34. *Winters v. New York*, 333 U.S. 507 (1948).

35. *Id.* at 508 (quoting N.Y. PENAL LAW § 1141 (McKinney 1946)).

36. *Id.* at 511.

37. *Id.* at 508 n.1.

38. *People v. Winters*, 48 N.Y.S.2d 230, 231 (N.Y. App. Div. 1944).

39. *Id.*

40. *Id.*

41. *Winters*, 333 U.S. at 510.

42. *Time, Inc. v. Hill*, 385 U.S. 374, 388 (1967).

43. *Smith v. Daily Mail Publ’g Co.* (“*Daily Mail*”), 443 U.S. 97 (1979).

44. *Fla. Star v. B.J.F.*, 491 U.S. 524, 536-37 (1989). In this case, a small Florida newspaper published a rape victim’s name despite a statute making such a publication a crime.

As the court synthesized in *Daily Mail*, “[o]ur recent decisions demonstrate that state action to punish the publication of truthful information seldom can satisfy constitutional standards.”<sup>45</sup> Detective stories, even scandalous and salacious ones, even ones involving identities of crime victims, identities of juvenile criminal defendants, and sensationalized details of crimes, were protected expression. The press that reported them, it seemed, was free.

## II. A PROSECUTOR’S FALL AND A MODEL’S MURDER: NEWS OR PUNISHABLE SENSATIONALISM?

In the years that followed earlier privacy scholarship, the publication of the Second Restatement, and the somewhat parallel reasoning protecting sensationalistic news media in Supreme Court jurisprudence regarding crime news, most news stories reporting crime events have been protected by courts. As painful as such stories may be for both perpetrators and victims, the “newspaper enterprise,” as Warren and Brandeis called it,<sup>46</sup> could report deeply and sometimes embarrassingly about criminal actors and even crime victims without fearing liability. When a perpetrator or a victim argued that the press had gone too far and brought a lawsuit for damages, such plaintiffs generally lost because the news media was able to shield itself with the First Amendment and argue that, above all, crime news is news and is, therefore, protected.

In very recent times, however, a handful of courts have troublingly questioned and criticized the depth of certain crime reporting. They have sided, sometimes surprisingly, with plaintiffs in cases that parallel some examples of what is considered appropriate coverage in the Restatement and elsewhere. In some of those decisions, the courts have held publications potentially liable for reporting things that seem to be somewhat routine detective stories.

Perhaps the best example of this is a case from a federal district court involving the *To Catch a Predator* segment of the *Dateline* television program that aired on NBC and continues in reruns. During the production of a typical *To Catch a Predator* episode, anchor Chris Hansen worked with the vigilante group that calls itself Perverted Justice and with local police. Each production was a televised sting operation: Perverted Justice workers and actors pretended to be young teenagers and posted chatty things online, occasionally reaching adults only too happy

---

The Court sided with the newspaper. See also *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 492 (1975), a case involving a rape and murder and the publication of the victim’s name, in which the Court found for the newspaper and wrote that the press brings the “beneficial effects of public scrutiny upon the administration of justice.”

45. *Daily Mail*, 443 U.S. at 102.

46. Warren & Brandeis, *supra* note 7, at 195.

to hit on them in cyberspace. These unsuspecting adults—overwhelmingly male and seemingly in droves, no matter the city in which the *To Catch a Predator* program was taped—communicated online with the “teens,” sometimes sending explicit photographs of their genitalia and often using explicit sexual language in suggesting a meeting at what they believed to be a house empty of anyone except the teenager. The Perverted Justice workers posing as children would then agree to meet the men. Much to the surprise of these suspected pedophiles, the house was wired for video and sound, NBC reporter Chris Hansen appeared instead of the child and confronted the men with transcripts of their online sex talk, and police arrested the men as they attempted to leave the home. Men caught in *To Catch a Predator* television episodes have included soldiers, police officers, teachers, a medical doctor, a minister, and a rabbi.<sup>47</sup>

In 2006, *To Catch a Predator* set up a sting in Murphy, Texas, north of Dallas. A man calling himself Wil—a 56-year-old who pretended to be a 19-year-old college student—contacted an actor who, with Perverted Justice’s guidance, pretended to be a lonely 13-year-old boy with divorced parents, a “neglectful” father, and a “no good” stepfather. The “boy” pretended to be accessing the Internet from a neighbor’s empty house where he was dog sitting.

At first, the online conversations between 56-year-old “Wil” and the “child” were friendly, but they soon turned sexual. Here are a few of the communications sent by the adult to the boy over the course of their two-week online relationship, as reported by *Esquire* magazine: “could I feel your cock”; “how thick are you”; “i want to feel your cock”; “maybe you can fuck me several times”; “has anyone sucked you”; and “just talking about this has me hard.” The man had confessed to the child at the computer that “he liked young boys.”<sup>48</sup>

This 56-year-old man was a surprising suspect, even for the seasoned *To Catch a Predator* workers: he was William Conratt, a Texas prosecutor, the chief felony officer for a nearby county. He had once run unsuccessfully for a county judgeship. “Wil” had given the boy enough information about him so that he was easily outed as Conratt by Perverted Justice researchers behind the scenes.

Communicating with an underage person on the Internet in a sexual manner is a crime in itself, and the police and *To Catch a Predator* producers eventually went to Conratt’s house to arrest him. Conratt apparently realized that an arrest was imminent and shot himself as

---

47. For a somewhat biased description of the Perverted Justice process, see Luke Dittrich, *Tonight on Dateline This Man Will Die*, *ESQUIRE*, Sept. 1, 2007, at 232. The facts described herein are taken from this magazine article.

48. *Id.*

police entered his home. He died from a self-inflicted gunshot wound to the head.

As I have suggested previously,<sup>49</sup> there is no question that it is important news when a prosecutor breaks the law, even if the law that is broken is one with no physical victim other than society as a whole. Prosecutors take an oath to uphold the law and protect citizens, so when that oath is broken, constituents deserve to know about the criminal violation and it necessarily makes headlines.

When the law that a prosecutor breaks involves a potential sexual encounter with a child—a crime of an extraordinarily harmful sort—the news value of the story and the public’s need to know is that much greater. Before his own fall from grace and suicide, in fact, Prosecutor Conradt had been interviewed in a news story about a preschool teacher’s arrest on sexual abuse charges.<sup>50</sup> If it was news (news that Conradt himself obviously embraced) that a preschool teacher had been arrested, there is no question that it was news that a prosecutor would be charged as part of a sting against pedophiles.

But in the case stemming from NBC’s news coverage, one filed by Conradt’s sister claiming that the prosecutor suffered intentional infliction of emotional distress at the hands of the *Dateline NBC* journalists, the federal trial court judge saw little or no news value in the story that a prosecutor allegedly broke the law by using strongly sexual language while communicating with a person he thought was a 13-year-old boy. Instead, in an opinion that does not include the language written by Conradt to the child, the judge strongly criticized NBC for putting Conradt in the position that it had, concluding that “reasonable minds could differ as to whether NBC’s conduct was so ‘outrageous and extreme’ as to exceed all possible bounds of decency” and deciding against NBC in its motion to dismiss the proceedings.<sup>51</sup>

A jury, the judge explained, could decide that what happened to Conradt was not news and that NBC was in a unique “position of power” to recognize that Conradt would be emotionally harmed by NBC’s actions.<sup>52</sup> Suddenly, the crime reporting recognized as absolutely legitimate by the Restatement authors and Supreme Court justices had suffered a serious setback.

Moreover, the court used highly abstract journalism ethics provisions against NBC. The opinion includes principles from the

---

49. Amy Gajda, *Judging Journalism: The Turn Toward Privacy and Judicial Regulation of the Press*, 97 CAL. L. REV. 1039 (2009).

50. Bill Lodge, *Ex-Mabank Teacher is Named in Abuse Suit*, DALLAS MORNING NEWS, Sept. 22, 1993, at 31A.

51. Conradt v. NBC, 536 F. Supp. 2d 380, 396 (S.D.N.Y. 2008).

52. *Id.* at 397.

Society for Professional Journalists' Code of Ethics and finds that not only could NBC be liable for violating them, but that such violations could be the basis for the intentional infliction of emotional distress claim.<sup>53</sup>

Such a decision is especially troubling because the ethics provisions on which the court relied are purposefully ethereal, incapable of objective definition, and not mandatory. These provisions include the highly subjective suggestion that journalists "[s]how good taste [and] [a]void pandering to lurid curiosity."<sup>54</sup> *Dateline's To Catch a Predator*, the judge wrote, could be liable because a reasonable jury could find that it failed to show good taste and pandered to lurid curiosity in its coverage of *Conrad*.<sup>55</sup> NBC, the judge suggested, had taken on a cause, had "fail[ed] to be judicious about publicizing allegations before the filing of charges," and had not lived up to journalism's ethics principles by making news instead of reporting it.<sup>56</sup> The court walked through the journalistic analysis and decided for itself that the news of a prosecutor's arrest is of no news value.

Moreover, the language in the decision is arguably broad enough to allow any judge to cast a critical eye and analyze nearly every on-the-scene news story involving crime in the same way. As long as reporters are tipped off by police, it seems, under the *Conrad* decision, a reasonable jury could find a valid intentional infliction of emotional distress claim based on the news media's failure to show good taste, its pandering, its lack of judiciousness, and its creating, rather than reporting, news.

It is also remarkable that the trial court decision in *Conrad* contradicts decades of privacy law. Certainly the arrest of a prosecutor on child sex charges is the sort of "public interest" news Warren and Brandeis hinted at in 1890 when they suggested that some news would in fact be in the public interest, and what Prosser had suggested more strongly in 1960 when he purposefully included crime within his definition of matters of popular appeal. It also completely contradicts the way in which the Restatement defines news today when it lists crime stories as newsworthy matters, even if they are of more or less deplorable popular appeal. But in allowing the intentional-infliction-of-emotional-distress case to go forward, the trial court judge very clearly rejected those broad and traditional—in both a legal and a journalistic sense—parameters of news. In fact, the decision allows for exactly the situation

---

53. *Id.* at 397-98.

54. *Id.* at 397 (quoting SOCIETY OF PROFESSIONAL JOURNALISTS, CODE OF ETHICS (1996), available at <http://www.spj.org/pdf/ethicscode.pdf>).

55. *Id.* at 398.

56. *Id.*

of which the Restatement authors warn: the successful stifling of news decidedly in the public interest by one who would “not only not seek publicity but [would] make every possible effort to avoid it,” i.e., the alleged perpetrator of a crime and his family.<sup>57</sup>

The *Conradt* decision is not the only recent case in which a court has sided with a plaintiff over news media in a crime-related news reporting case. A second example concerns the 2007 spousal murder of a female professional wrestler and *Hustler* magazine’s use of nude photos taken years before to illustrate its story about the murder.

In that case,<sup>58</sup> Christopher Benoit, also a professional wrestler, killed his wife, Nancy Benoit, and their child, and then committed suicide. Nancy Benoit had modeled in the years before her wrestling career and had posed nude for a photographer. After her murder, which was international news,<sup>59</sup> *Hustler* magazine published ten photographs from that nude sitting in two pages of its magazine. Nancy Benoit’s mother brought a right-to-publicity claim against *Hustler*.

Even though the right to publicity is a property-based action, it generally contains an exception for newsworthiness. In other words, if a photograph itself has news value or that photograph has a connection with a published and valid news story, a person featured in the photograph would have no viable claim for a property right in his or her image and would not have a viable action against media that published it: “[W]here the publication is newsworthy, the right of publicity gives way to freedom of the press.”<sup>60</sup>

The Eleventh Circuit decided the Benoit matter and necessarily had to consider the news value of the photographs and of the *Hustler* story itself. In a unanimous decision, the judges decided in favor of Nancy Benoit’s family and against *Hustler*.<sup>61</sup>

First, the court decided, the photographs had absolutely no news value themselves; the three judges suggested that had the photos been published by a magazine without an accompanying story, “the publication would not qualify within the newsworthiness exception” to the right to publicity in Georgia.<sup>62</sup> “Indeed,” the court wrote in explaining its news judgment regarding the photographs, “people are nude every day, and the news media does not typically find the occurrence worth reporting.”<sup>63</sup>

Second, the court held, the news story that accompanied the

---

57. RESTATEMENT (SECOND) OF TORTS § 652D cmt. f (1977).

58. *Toffoloni v. LFP Publ’g Grp., LLC*, 572 F.3d 1201, 1204 (11th Cir. 2009).

59. *Id.* at 1204, 1209.

60. *Id.* at 1208.

61. *Id.* at 1213.

62. *Id.* at 1209.

63. *Id.*

photos—a “brief biography”—was “merely incidental” to the publication of the photographs, and, therefore, could not itself make the nude photographs into anything of news value.<sup>64</sup> The biography may have had some news value alone but not enough to bring the photographs into the newsworthiness exception, the court decided, despite the fact that the article specifically mentioned Ms. Benoit’s modeling days and focused on her life story.

Finally and most troublingly, the court wrote that it was convinced that the nude photos were not connected to any matter of public concern.<sup>65</sup> Interpreting Georgia law, it suggested that “timeliness” and “relatedness boundaries” could put an end to public scrutiny even when an incident may be one in the public interest.<sup>66</sup> The court explained,

[Hustler] would have us rule that someone’s notorious death constitutes a carte blanche for the publication of any and all images of that person during his or her life, regardless of whether those images were intentionally kept private and regardless of whether those images are of any relation to the incident of public concern. We disagree.<sup>67</sup>

The court then turned to the Restatement and offered its own assessment of the newsworthiness provisions under these facts. It focused on language that suggests that some actresses may keep some matters private, that news ends when it becomes morbid and sensational prying for its own sake, and that the newsworthiness of a story ends when those with decency would have no interest in it.<sup>68</sup> The court then explained that, under reasoning based upon the Restatement, the photographs “in no conceivable way” related to the murder.<sup>69</sup> “The photographs bear no relevance” to the news story, the court wrote, and explained that it worried that should it decide the case any other way, all magazines “would be free to publish any nude photographs of almost anyone without their permission, simply because the fact that they were caught nude on camera strikes someone as ‘newsworthy.’”<sup>70</sup>

The court closed its opinion with a brief paragraph repeating its decision that the photos did not qualify for the right to publicity’s exception for newsworthiness: “These private, nude photographs were not incident to a newsworthy article; rather, the brief biography was

---

64. *Id.* at 1210.

65. *Id.* at 1212.

66. *Id.* at 1210.

67. *Id.*

68. *See id.* at 1211.

69. *Id.*

70. *Id.* at 1212.

incident to the photographs” and “these photographs were neither related in time nor concept to the current incident of public interest.”<sup>71</sup>

What is remarkable about the *Benoit* case is not so much its decision that a right to publicity existed in the photographs of Nancy Benoit or that the magazine seemed to have created a story in an effort to use the images. Instead, it is the strength of the court’s language that the photographs rated an absolute zero on any conceivable news value scale. The photos, in the court’s mind, bore “no relevance” to news and were completely unrelated to anything that had been reported in the news media, despite the fact that the murders made international headlines and even though the court found Nancy Benoit to be a public figure.<sup>72</sup>

The trial court hearing the case would later quote experts who opined that Ms. Benoit was such a “celebrity,” in fact, that the photographs themselves would be valued at up to \$200,000 and that by publishing the photos *Hustler* had ruined the market for a tribute DVD that could have brought nearly \$300,000 in profits to Nancy Benoit’s estate.<sup>73</sup> These are indeed remarkable sums for photographs that the appeals court found had absolutely no news value.

It is also remarkable that the court would find Ms. Benoit’s life story, at least in the court’s concluding language, not newsworthy. Clearly there is some value to the life story of someone who is murdered, given that such news coverage is routine in news media today and given that the story of Benoit’s own murder became international news.

Moreover, there is at least some potential journalistic link between the nude photographs and the news article—one the court complained took up only one-sixth of the two-page spread. Any life story of a celebrity would necessarily include the celebrity’s past, and that past would include some embarrassing moments, including decisions made for publicity’s sake alone. Here, the fact that Ms. Benoit posed nude may have indicated at least an initial strong desire on her part for any and all publicity, something that may explain her involvement with professional wrestling and ultimately the professional wrestler who became her husband and murderer. The fact that she posed nude, even if she later changed her mind, may reveal an important and relevant dimension to her life. It may also evidence the sometimes-held belief that women must take off their clothing to achieve celebrity. This link between the photos and something more acceptably newsworthy gives some potential news value, albeit minimal, to the photos themselves. As the Restatement authors repeatedly note, but as the judge in the *Benoit*

---

71. *Id.* at 1213.

72. *See id.* at 1212.

73. *Toffoloni v. LFP Publ’g Grp.*, No. 1:08-CV-421-TWT, 2010 U.S. Dist. LEXIS 124733, at \*5-6 (N.D. Ga. Nov. 23, 2010).

case overlooked, crime victims have sadly become a part of our local or even national dialogue. Inquiry into their lives—including inquiry into events outside of the crime itself—is an appropriate part of the news and, therefore, protected by the First Amendment.<sup>74</sup>

This is, of course, not to suggest that *Hustler* made the correct, ethical decision to publish the photographs, or that people have no right to bring claims based upon publication of certain nude photographs. What it does suggest is that the court went unnecessarily far when it wrote that the story was not newsworthy and that the photos had no news value whatsoever. The court leapt to characterize the images as those in which only persons without any sense of decency would be interested. *Hustler*, at least, believed that many persons would be interested in the story and, admittedly, the photos; the court itself noted as much when it quoted the headlines on the magazine's cover. Are these people at whom the headlines were aimed the mysterious people without a sense of decency who do not understand what real news is? Is their interest instead morbid and sensational prying for its own sake? Do we lump anyone interested in learning of Nancy Benoit's decision to take nude photos into the group that Warren and Brandeis believed required a more cultured guiding hand in news decisions? Would a mention in a news story of such a nude photo session be a privacy invasion?

And, finally, is this story of a murder and nude photographs the sort of thing that is decidedly morbid and sensational prying for its own sake? Or it is simply one of those things that is, under the First Amendment, of more or less deplorable popular appeal and, therefore, protected?

Because these questions are not answered in any way that protects news publications, the *Benoit* decision too could have a chilling effect. It holds that there are some things from a celebrity crime victim's past that are off limits, even when photographs of the event or events exist. Any wise news editor, it seems, should think twice before publishing decades-old photographs of a celebrity, as there is a possibility that a court could find them both not newsworthy and unrelated to the underlying news story. Because involuntary public figures have an even greater right to privacy, that same editor would also be wise to consider carefully any photograph from a crime victim's past given the court's broad rejection of the photographs' news value in *Benoit*.

The opinion then, though deciding a seemingly property-rights-oriented, right-to-publicity matter, can be read far more broadly and could have a crushing effect on news media. The opinions in the *Conradt* and *Benoit* cases also suggest that courts are feeling far freer to decide the news value of all stories, including those involving crime and including

---

74. RESTATEMENT (SECOND) OF TORTS § 652D, cmt. f (1977).

those with accompanying photographs or video.

Two recent additional examples from Chicago are similarly telling and troubling. Chicago is one of the nation's largest cities and one in which crime is reported heavily on a daily basis. One federal judge there, however, rejected a motion to dismiss in a case involving a woman whose arrest was depicted on a reality television program; the woman's intentional infliction of emotional distress claim was based in part upon the broadcast of her arrest and the way police described her as a "[p]retty little blond[e] girl . . . driving a Jaguar."<sup>75</sup> And in a newsgathering case, a federal trial court judge decided that journalists could potentially be liable for the privacy tort of intrusion because they had used a telephoto lens to record people in a fenced backyard. The persons recorded included a reporter fraternizing with a man then believed to be involved in the disappearance of his wife, one of the biggest news stories of the summer. The court wrote that a reasonable jury could find that the videotaping of the event was extreme and outrageous conduct—even though it took place on the man's sister's property, even though the man himself was present, and even though the event took place outside.<sup>76</sup>

What unites all of these recent cases is an underlying detective story. And even though these detective tales of true crime have routinely been protected by scholars and courts as those most newsworthy and most in the public interest, recently courts have, at least initially, ruled against the media.

### III. A CHILL IN REPORTING CRIME NEWS

It seems as if it should be completely unnecessary to argue that detective stories are especially protected under the First Amendment. Even Samuel Warren and Louis Brandeis, certainly no fans of news media, recognized that at some point the public's interest in a particular news story outweighs the privacy sought by those involved. That's all the more true in a criminal matter, one directly affecting the public in its prosecution, one that violates the law put in place for the protection of the public, and one that is routinely of great public interest.

---

75. *Best v. Malec*, No. 09 C 7749, 2010 U.S. Dist. LEXIS 58996, at \*5, \*17-18 (N.D. Ill. June 11, 2010).

76. *Webb v. CBS*, No. 08 C 6241, 2009 U.S. Dist. LEXIS 38597, at \*12 (N.D. Ill. May 7, 2009). Perhaps it is not surprising that these cases come from Illinois, given that a few years before, an appeals court found that a plaintiff had a valid privacy claim after a news article about crime statistics in Chicago included a photograph of her murdered son and the words she spoke over his dead body. *Green v. Chi. Tribune*, 675 N.E. 2d 249 (Ill. App. Ct. 1996). A California court followed a few years later and criticized news reporting in *Sports Illustrated* about adult coaches who sexually abused child players. The article included a Little League team photograph picturing some members who had been molested by their coach. *M.G. v. Time Warner*, 89 Cal. App. 4th 623 (Cal. Ct. App. 2001).

And yet today, it seems, courts are increasingly skeptical about such news coverage. The *Conradt* court wrote explicitly that a jury could decide that NBC had overstepped its bounds and caused a would-be arrestee great emotional distress by showing up and reporting at the arrestee's home; the jury could find NBC liable for intentional infliction of emotional distress because it violated some ethereal journalistic ethics provisions to be, in a word, nice.

If a line is to be drawn—and the Supreme Court has yet to tell us with uniformity if such a line is constitutionally permissible and, if so, where news ends and an invasion into private matters begins—it is surely not in the case of a prosecutor who, it seems, strongly and repeatedly hit on, using graphic sexual terms, a person he presumably thought to be a 13-year-old boy. It violates the First Amendment and chills news reporting to hold media liable for a failure to be nice, especially in a situation involving the arrest of a public official, especially in coverage of a detective story.

And yet, given these decisions, imagine the news editor who must make the call about coverage of a particular crime story. If that news editor is to be sure that such coverage will be in line with existing law and will avoid any potential for liability, that coverage should not violate any of journalism's highly subjective, ethereal, and aspirational ethics provisions. That editor must also consider the ways in which a lay judge or jury might interpret such ethics provisions.

Imagine the questions that might be included in a news editor's analysis:

Would a court consider it advocacy or news reporting to cover an arrest if the media is tipped off by the police?

Is it a violation of the ethics provision that suggests that reporters "recognize that gathering and reporting information may cause harm or discomfort" if the news story suggests that a public official may have broken the law?

Would it be in good taste and not pander to lurid curiosity to report details of a public official's criminal attempts to communicate with a young child using graphic sexual language, including the suggestion that the prosecutor wished to feel that child's "cock"?

Should the publication include what might be considered potentially embarrassing photos taken many years before that a court could find lacked news value and a real connection to the underlying story of a crime?

Before *Conradt* and the decision in the *Benoit* case, the answers

would be clear and the news editor could move forward with covering the story. Today, the answers are not so clear and it is easy to use the word “chilling” when considering a newsroom analysis of coverage, especially in an age when news media have few financial resources to defend against legal actions and instead may decide it safer not to report the news story involving crime at all.

Finally, and as William Prosser and others have noted, what person who is arrested or is otherwise involved in some way in a crime news story would not want privacy? Reading *Conradt* and the other decisions broadly, multiple arrestees and others could have a valid claim for intentional infliction of emotional distress should their arrests be reported, even if they are public officials. There is absolutely no doubt that reporting on any such matter causes harm and discomfort to the arrestee.

I am concerned that these decisions condemning media could increase and that courts could tighten even further their definition of “news” to exclude certain crime details. A California appeals court in early 2010, for example, held police responsible for publishing on the Internet death images of a young woman killed in an accident.<sup>77</sup> The court called the spread of the images across the Internet “a malignant firestorm” and lamented that the images appeared on thousands of websites, spread around the world via e-mail, and led to the family’s great emotional harm.<sup>78</sup> The court called it “Internet sensationalism” and “lurid gossip[,]” and its desire to protect surviving family members from such emotional trauma was clear.<sup>79</sup> A concurring judge in the three-judge decision wrote explicitly that surviving family members should have a right to their own privacy in any death images taken at an accident scene or at an autopsy.<sup>80</sup>

A continued backlash against this type of publishing could lead to additional cases that further quash the reporting of detective stories by traditional media.

## CONCLUSION

It is not surprising that certain courts hold certain media responsible for certain irresponsible reporting, especially today when the Internet routinely pushes the envelope. What is surprising is that some recent courts have punished media in the context of crime reporting, a type of reporting routinely protected by courts under the First Amendment and

---

77. *Catsouras v. Dep’t of Cal. Highway Patrol*, 181 Cal. App. 4th 856, 863–64 (Cal. Ct. App. 2010).

78. *Id.* at 863.

79. *Id.* at 864.

80. *Id.* at 898, 903.

by commentators since at least the time of Warren and Brandeis. News publications report on crime daily in many cities across the United States, and people read those stories in droves, proof that such reporting is in the public interest.

As the Supreme Court reiterated recently in *Snyder v. Phelps*,<sup>81</sup> “[s]peech deals with matters of public concern when it can ‘be fairly considered as relating to any matter of political, social, or other concern to the community,’ or when it ‘is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public,’ . . . [and t]he arguably ‘inappropriate or controversial character of a statement is irrelevant to the question whether it deals with a matter of public concern.’”<sup>82</sup>

Courts should recognize anew the value of detective stories and protect this type of journalistic coverage especially.

---

81. *Snyder v. Phelps*, 131 S. Ct. 1207 (2011).

82. *Id.* at 1216 (internal citations omitted).

# PUBLIC FIGUREHOOD IN THE DIGITAL AGE

DAVID LAT AND ZACH SHEMTOB\*

INTRODUCTION..... 403

I. THE PUBLIC FIGURE CONCEPT IN DEFAMATION LAW:  
FROM NEW YORK TIMES TO GERTZ ..... 404

II. THE ROAD NOT TAKEN: ROSENBLOOM V. METROMEDIA . 408

III. WHY ROSENBLOOM, NOT GERTZ, OFFERS THE BEST  
STANDARD FOR DECIDING DEFAMATION CLAIMS IN  
THE DIGITAL AGE. .... 410

    A. *Changes in the media landscape have undermined Gertz’s  
“self-help” rationale.*..... 410

    B. *The digital age has significantly eroded the “public figure”  
versus “private figure” distinction.* ..... 412

    C. *Objections to adoption of the Rosenbloom rule can be  
overcome.*..... 416

CONCLUSION..... 418

## INTRODUCTION

“I’M FAMOUS – on MySpace.”<sup>1</sup>

The T-shirt slogan may be tongue-in-cheek, but it reflects an important truth: the digital age, marked by the rise of new media and social networking, is radically transforming what it means to be “famous.”<sup>2</sup> What implications does this have for the legal understanding of what it means to be a public figure?

The concept of “public figurehood” has been explored most extensively in the context of defamation law.<sup>3</sup> In the landmark case of

---

\* David Lat is the founder and managing editor of the legal website Above the Law. Zachary Shemtob is an Assistant Professor in Criminal Justice and Criminology at Central Connecticut State University.

1. I’m Famous on Myspace T-shirts, Zazzle.com, [http://www.zazzle.com/im\\_famous\\_on\\_myspace\\_tshirt-235471316444495429](http://www.zazzle.com/im_famous_on_myspace_tshirt-235471316444495429) (last visited May 23, 2011).

2. Rex Sorgatz, *The Microfame Game*, N.Y. MAG., June 17, 2008; Clive Thompson, *Clive Thompson on The Age of Microcelebrity: Why Everyone’s a Little Brad Pitt*, WIRED, Dec. 2007, at 84; Jason Tanz, *Almost Famous*, WIRED, Aug. 2008, at 107.

3. This certainly has implications outside of the defamation context, most notably with respect to privacy torts, but we confine our analysis here to libel and slander.

*New York Times Co. v. Sullivan*,<sup>4</sup> the Supreme Court ruled that public officials must establish “actual malice” when suing for defamation. A second major case in this area, *Gertz v. Robert Welch, Inc.*, holds that the *New York Times* rule applies not just to public officials, but to “public figures” as well.<sup>5</sup> *Gertz*—as interpreted and applied by lower courts as the basis for developing various tests for public figurehood—continues to be good law.

As we shall argue, profound changes to the media landscape have rendered *Gertz* obsolete. We do not develop a new standard from whole cloth, however, but believe that Justice Brennan’s plurality opinion in *Rosenbloom v. Metromedia*,<sup>6</sup> decided several years before *Gertz*, provides a superior framework for approaching defamation claims in the digital age.

The question of who is or is not a public figure, far from being an abstract academic inquiry, has very real implications for the media, old and new alike, and for public discourse. In the words of Justice Brennan, “the rules we adopt to determine an individual’s status as ‘public’ or ‘private’ powerfully affect the manner in which the press decides what to publish and, more importantly, what not to publish.”<sup>7</sup>

In Part I, we review the relevant case law concerning who constitutes a public figure. In Part II, we provide a more detailed discussion of the *Rosenbloom* case. In Part III, we explain why Justice Brennan’s opinion in *Rosenbloom* is particularly well-suited for addressing public figurehood in a world of instant and pervasive communication.

## I. THE PUBLIC FIGURE CONCEPT IN DEFAMATION LAW: FROM NEW YORK TIMES TO GERTZ

Before we turn to focus specifically on *Gertz*, *Rosenbloom*, and their divergent approaches to public figurehood, a brief survey of the key Supreme Court decisions is in order. This background will make clear why public figure status matters and how the concept has evolved in the case law over time.

In 1964, in *New York Times Co. v. Sullivan*,<sup>8</sup> the Supreme Court set forth important First Amendment limitations on the defamation torts of libel and slander. The Court held that public officials cannot recover

4. *New York Times Co. v. Sullivan*, 376 U.S. 254, 282 (1964).

5. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974).

6. *Rosenbloom v. Metromedia Inc.*, 403 U.S. 29 (1971).

7. *Lorain Journal Co. v. Milkovich*, 474 U.S. 953, 954 (1985) (Brennan, J., dissenting from denial of certiorari); see also Rodney A. Smolla & W. Coleman Allen, *Statement from Iseman’s Lawyers*, N.Y. TIMES, Feb. 19, 2009, available at <http://www.nytimes.com/2009/02/20/business/media/20lawyers.html#> (arguing that the issue of who is a public figure “deserves ongoing scrutiny, certainly in our schools of law and journalism, but also in the arena of public debate”).

8. *New York Times*, 376 U.S. at 266.

damages for defamation absent proof that the statement in question was made with “actual malice.” In his opinion, a ringing endorsement of free speech values in a democracy, Justice Brennan wrote:

The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with “actual malice”—that is, with knowledge that it was false or with reckless disregard of whether it was false or not.<sup>9</sup>

This was a profoundly important development, as explained by Judge Robert D. Sack:

Against the backdrop of centuries of Anglo-American law permitting regulation of speech to protect reputation, this statement—protecting speech about public matters irrespective of its impact on reputation—was revolutionary. . . . It set a single standard for libel suits by public officials against the press in every court in the nation. Implicitly, it subjected all actions for defamation to constitutional scrutiny.<sup>10</sup>

The plaintiff in *New York Times* was a public official (L.B. Sullivan, one of three elected city commissioners in Montgomery, Alabama).<sup>11</sup> In the 1967 case of *Curtis Publishing Co. v. Butts*,<sup>12</sup> the Court extended the *New York Times* rule to “public figures” as well as public officials. The case involved a private individual, a university athletic director and former head football coach, who was accused in a newspaper article of conspiring to fix a football game. The Court issued a confusing raft of separate opinions in *Curtis*, but in a concurrence in the result, which was controlling on this issue, Chief Justice Warren expressed the view that the *New York Times* standard should apply to cases involving “public figures” as well as “public officials.”<sup>13</sup> As Chief Justice Warren sensibly noted, “differentiation between ‘public figures’ and ‘public officials’ and adoption of separate standards of proof for each have no basis in law, logic, or First Amendment policy. Increasingly in this country, the distinctions between governmental and private sectors are blurred.”<sup>14</sup>

Due to the fragmentation of the Court, *Curtis* did not generate a definitive rule on applicability of the *Times* standard to plaintiffs who are

---

9. *Id.* at 279-80.

10. ROBERT D. SACK, SACK ON DEFAMATION: LIBEL, SLANDER & RELATED PROBLEMS § 1:2.2 (4th ed. 2010).

11. *New York Times*, 376 U.S. at 256.

12. *Curtis Publ'g Co. v. Butts*, 388 U.S. 130, 155 (1967).

13. *Id.* at 164 (Warren, C.J., concurring in the result).

14. *Id.* at 163.

not public officials. That ruling came several years later, when the Court decided *Gertz*<sup>15</sup>—which remains the governing law in this area some thirty-five years later.

As set forth in Justice Powell's opinion for the Court, *Gertz* presented "the extent of a publisher's constitutional privilege against liability for defamation of a private citizen."<sup>16</sup> The *Gertz* Court held that the "actual malice" rule of *New York Times* does not apply to private persons (in this case, an attorney who represented a party in high-profile litigation).

Justice Powell noted that "[t]heoretically, of course, the balance between the needs of the press and the individual's claim to compensation for wrongful injury might be struck on a case-by-case basis."<sup>17</sup> But such an approach would present the following difficulty:

[It] would lead to unpredictable results and uncertain expectations, and it could render our duty to supervise the lower courts unmanageable. Because an ad hoc resolution of the competing interests at stake in each particular case is not feasible, we must lay down broad rules of general application. Such rules necessarily treat alike various cases involving differences as well as similarities. Thus it is often true that not all of the considerations which justify adoption of a given rule will obtain in each particular case decided under its authority.<sup>18</sup>

In other words, the *Gertz* approach finds some of its justification in concerns of efficiency and ease of application.

In reaching the conclusion that private-figure plaintiffs should not have to comply with the rigorous *New York Times* standard when suing for defamation, the *Gertz* Court drew distinctions between different types of defamation plaintiffs. It began with what could be described as *Gertz's* first rationale:

The first remedy of any victim of defamation is self-help—using available opportunities to contradict the lie or correct the error and thereby to minimize its adverse impact on reputation. Public officials and public figures usually enjoy significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements than private individuals normally enjoy. Private individuals are therefore more vulnerable to injury, and the state interest in protecting them is correspondingly greater.<sup>19</sup>

---

15. *Gertz v. Robert Welch, Inc.*, 418 U.S. 334 (1974).

16. *Id.* at 325.

17. *Id.* at 343.

18. *Id.* at 343-44.

19. *Id.* at 344.

It then offered a second justification:

[T]he communications media are entitled to act on the assumption that public officials and public figures have voluntarily exposed themselves to increased risk of injury from defamatory falsehood concerning them. No such assumption is justified with respect to a private individual. . . . [P]rivate individuals are not only more vulnerable to injury than public officials and public figures; they are also more deserving of recovery.<sup>20</sup>

In light of these differences, the *Gertz* Court declined to extend the *New York Times* standard to defamation suits brought by private individuals.

Having concluded that the *Times* rubric applies only to suits brought by public figures, the *Gertz* Court identified two ways of attaining public figure status:

In some instances an individual may achieve such pervasive fame or notoriety that he becomes a public figure for all purposes and in all contexts. More commonly, an individual voluntarily injects himself or is drawn into a particular public controversy and thereby becomes a public figure for a limited range of issues.<sup>21</sup>

The first designation describes a “pervasive” or “all-purpose” public figure, and the second designation describes a “limited purpose” public figure.<sup>22</sup> In determining whether a private individual should be subject to the *New York Times* “actual malice” standard, a court must consider the “nature and extent of an individual’s participation in the particular controversy giving rise to the defamation.”<sup>23</sup>

Taken together, *New York Times* and *Gertz* provide much of the framework against which defamation claims are evaluated today. As noted by Judge Sack, “[t]he *New York Times* and *Gertz* cases have affected the vast majority of defamation cases decided after them,” with state and lower federal courts filling in many of the gaps left by these cases.<sup>24</sup>

---

20. *Id.* at 345. A somewhat crisper formulation was offered by the Supreme Court in *Wolston v. Reader’s Digest Ass’n, Inc.*, 443 U.S. 157, 164 (1979): “[P]ublic figures are less deserving of protection than private persons because public figures, like public officials, have ‘voluntarily exposed themselves to increased risk of injury from defamatory falsehood concerning them.’”

21. *Gertz*, 418 U.S. at 351.

22. SACK, *supra* note 10, § 1:5 at 1-33 to -34.

23. *Gertz*, 418 U.S. at 352.

24. SACK, *supra* note 10, § 1:2.6 at 1-20. For example, based on *Gertz*, lower courts have developed tests for limited-purpose public figure status. *See, e.g.*, *Carr v. Forbes, Inc.*, 259 F.3d 273, 280 (4th Cir. 2001) (utilizing a five-factor test).

## II. THE ROAD NOT TAKEN: ROSENBLUM V. METROMEDIA

In the decade between *New York Times*, decided in 1964, and *Gertz*, decided in 1974, the Supreme Court decided the case of *Rosenbloom v. Metromedia, Inc.*<sup>25</sup> In his plurality opinion, Justice Brennan described the issue presented in *Rosenbloom* as follows: “whether the *New York Times*’ knowing-or-reckless-falsity standard applies in a state civil libel action brought not by a ‘public official’ or a ‘public figure’ but by a private individual for a defamatory falsehood uttered in a news broadcast by a radio station about the individual’s involvement in an event of public or general interest.”<sup>26</sup>

As in *Curtis Publishing*, the Court in *Rosenbloom* was fragmented, with no opinion garnering a majority of the justices. In a plurality opinion, representing the views of three justices, Justice Brennan rejected the distinction between public and private figures in the defamation context, expressing the view that the *New York Times* standard should apply to all reports of events of “public or general concern.”<sup>27</sup> But because Justice Brennan in *Rosenbloom* was joined by only two other justices, his opinion did not represent a definitive pronouncement by the Court on whether the rule of *New York Times* applies to defamation suits brought by private individuals. As a result, *Gertz*—in which the Court tackled essentially the same issue, but with an opinion that spoke for a majority of the Court—essentially supplanted Justice Brennan’s *Rosenbloom* opinion as the controlling framework.

Justice Brennan articulated the following rule in *Rosenbloom*: “We honor the commitment to robust debate on public issues, which is embodied in the First Amendment, by extending constitutional protection to all discussion and communication involving matters of public or general concern, without regard to whether the persons involved are famous or anonymous.”<sup>28</sup> Because it does not draw distinctions between types of plaintiffs, this rule is clearer and easier to apply than what would later replace it in *Gertz*.

The *Rosenbloom* plurality reached its conclusion through the following reasoning:

1. Free speech is critical to a self-governing society, and it reaches “all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.”<sup>29</sup>

---

25. 403 U.S. 29 (1971).

26. *Id.* at 31-32.

27. *Id.* at 52.

28. *Id.* at 43-44.

29. *Id.* at 41 (citing *Thornhill v. Alabama*, 310 U.S. 88, 102 (1940)).

2. The distinction between “public” and “private” is eroding/increasingly blurred.<sup>30</sup>

3. Freedom of the press isn’t just about political speech. “Comments in other cases reiterate this judgment that the First Amendment extends to myriad matters of public interest.”<sup>31</sup>

4. It makes little sense for free speech guarantees to turn on the fame or obscurity of the individuals involved:

If a matter is a subject of public or general interest, it cannot suddenly become less so merely because a private individual is involved, or because in some sense the individual did not ‘voluntarily’ choose to become involved. The public’s primary interest is in the event; the public focus is on the conduct of the participant and the content, effect, and significance of the conduct, not the participant’s prior anonymity or notoriety.<sup>32</sup>

Accordingly, Justice Brennan concluded that constitutional protection applies “to all discussion and communication involving matters of public or general concern, without regard to whether the persons involved are famous or anonymous.”<sup>33</sup>

Justice Brennan then proceeded to refute the arguments of the petitioner. He rejected the distinction between “public” and “private” figures in the First Amendment context:

Drawing a distinction between ‘public’ and ‘private’ figures makes no sense in terms of the First Amendment guarantees. The New York Times standard was applied to libel of a public official or public figure to give effect to the Amendment’s function to encourage ventilation of public issues, not because the public official has any less interest in protecting his reputation than an individual in private life. While the argument that public figures need less protection because they can command media attention to counter criticism may be true for some very prominent people, even then it is the rare case where the denial overtakes the original charge.<sup>34</sup>

He then made a broader argument about the elusive nature of “privacy”:

We have recognized that ‘(e)xposure of the self to others in varying degrees is a concomitant of life in a civilized community.’ Voluntarily or not, we are all ‘public’ men to some degree. Conversely, some aspects of the lives of even the most public men fall outside the area

---

30. *Id.* at 41-42.

31. *Id.* at 42.

32. *Id.* at 43.

33. *Id.* at 43-44.

34. *Id.* at 45-46.

of matters of public or general concern. Thus, the idea that certain ‘public’ figures have voluntarily exposed their entire lives to public inspection, while private individuals have kept theirs carefully shrouded from public view is, at best, a legal fiction.<sup>35</sup>

As we will explore in the next section, this argument has only grown stronger in the intervening years.

### III. WHY ROSENBLOOM, NOT GERTZ, OFFERS THE BEST STANDARD FOR DECIDING DEFAMATION CLAIMS IN THE DIGITAL AGE.

Widespread use of the Internet has rendered *Gertz* not only obsolete but legally incoherent for two primary reasons: (1) changes in the media landscape have undermined *Gertz*’s self-help rationale, and (2) the digital age has blurred, if not eliminated, the entire public/private distinction this case relied upon. While *Gertz* may have made sense in a particular social and historical context, Justice Brennan’s opinion in *Rosenbloom* holds far greater relevance today.

#### A. *Changes in the media landscape have undermined Gertz’s “self-help” rationale.*

The *Gertz* Court argued that public figures have better access to the channels of communication, and therefore a better ability to counteract false statements: “Private individuals are . . . more vulnerable to injury, and the state interest in protecting them is correspondingly greater.”<sup>36</sup> Based on this language from *Gertz*, lower courts determining public figure status would consider such factors as the individual’s “access to channels of effective communication.”<sup>37</sup>

This analysis reflects a very different—and outdated—media environment. When *Gertz* was decided in 1974, false charges could only be countered through access to a printing press, radio station, or television network—modes of communication that ordinary citizens generally could not tap into. In 2011, however, methods of communication have expanded and changed dramatically. Thanks to the phenomenon of blogging and the rise of social networks like Twitter and Facebook, ordinary citizens have historically unprecedented access to effective communication channels. One can refute false charges not just through newspapers, radio, or television, but through a proliferation of online outlets as well. Aggrieved subjects of media coverage no longer

---

35. *Id.* at 47-48 (internal citations omitted).

36. *Gertz*, 418 U.S. at 344.

37. *E.g.*, *Hatfill v. New York Times Co.*, 532 F.3d 312, 319 (4th Cir. 2008).

need a newspaper to print retractions of letters to the editor; instead, these subjects can go out and tell their own side of the story on a blog or social networking site.<sup>38</sup> (Indeed, if false rumors started online, refuting them online may be the most effective response.)

Because the marketplace of ideas is so robust in the digital age, greater freedom can be granted to the media, both old and new. The constitutional relevance of such changes in the media environment was recognized by justices even prior to *Gertz*. For example, Justice Harlan, whose jurisprudence was frequently less press-friendly than that of some of his colleagues, acknowledged that “falsehood is more easily tolerated where public attention creates the strong likelihood of a competition among ideas.”<sup>39</sup>

Of course, even in the digital age, famous celebrities still have greater access to communication channels than ordinary citizens. For example, Ashton Kutcher has more than six million followers on Twitter,<sup>40</sup> while the average Twitter user has only 126 followers.<sup>41</sup> Yet this still fails to legitimate *Gertz*’s rationale. First, perfect equality is not required. In the words of Justice Marshall:

[D]ifficulty in reaching all those who may have read the alleged falsehood surely ought not preclude a finding that [the plaintiff] was a public figure under *Gertz*. *Gertz* set no absolute requirement that an individual be able fully to counter falsehoods through self-help in order to be a public figure. We viewed the availability of the self-help remedy as a relative matter in *Gertz*, and set it forth as a minor consideration in determining whether an individual is a public figure.<sup>42</sup>

---

38. This enhanced ability to refute allegations may be relatively new. But the importance of the “privilege of reply, also known as the privilege to speak in self-defense or to defend one’s reputation,” traces its roots back to the common law. *Foretich v. Capital Cities/ABC, Inc.*, 37 F.3d 1541, 1559 (4th Cir. 1994).

39. *Time, Inc. v. Hill*, 385 U.S. 374, 407 (1967) (Harlan, J., concurring in part and dissenting in part); see also *New York Times Co. v. Sullivan*, 376 U.S. 254, 304 (1964). (Goldberg, J., concurring in the result) (“The conclusion that the Constitution affords the citizen and the press an absolute privilege for criticism of official conduct does not leave the public official without defenses against unsubstantiated opinions or deliberate misstatements. ‘Under our system of government, counterargument and education are the weapons available to expose these matters, not abridgment . . . of free speech . . .’” (quoting *Wood v. Georgia*, 370 U.S. 375, 389 (1962))).

40. See <http://twitter.com/Aplusk>.

41. Charles Arther, *Average Twitter User Has 126 Followers, and Only 20% of Users Go via Website*, GUARDIAN, (June 29, 2009, 3:24 PM), <http://www.guardian.co.uk/technology/blog/2009/jun/29/twitter-users-average-api-traffic>.

42. *Time, Inc. v. Firestone*, 424 U.S. 448, 486 (1976) (Marshall, J., dissenting); see also *Carr v. Forbes*, 259 F.3d 273, 282 n.2 (4th Cir. 2001) (“Of course, the Arizona and South Carolina media do not have the international readership of Forbes magazine. However, a court does not ask whether a defamation plaintiff has ever had access to a media outlet with the

Second, even if an aggrieved party might not initially have a large audience, reaching prominent speakers who do have sizable followings is no longer difficult. Thanks to advances in communications technology, getting one's side of the story before someone who does have a major bully pulpit might be as simple as sending an e-mail or "tweeting at" that individual. And the "crowdsourced" nature of news these days, in which thousands of citizen-journalists get involved in exploring all sides of an issue, also helps to ensure that multiple viewpoints are represented, especially with respect to the most controversial issues of the day.

The case of Shirley Sherrod, a former official at the U.S. Department of Agriculture, illustrates how disparities in access to media channels matter much less today than in the past. Sherrod had a much smaller audience than conservative activist Andrew Breitbart, publisher of the website BigGovernment.com, who posted portions of an edited video suggesting that Sherrod had acted in a racially discriminatory manner. In the ensuing controversy, Sherrod was forced to resign from her government job. Yet correcting the record in the digital age was easy: once the NAACP released the full video, Media Matters was quickly able to deconstruct the alleged smear campaign. This not only led to an apology to Sherrod from President Barack Obama and an offer to return to the Department of Agriculture from Secretary Tom Vilsack, but widespread sympathy for Sherrod's plight and outrage against Breitbart.<sup>43</sup>

*B. The digital age has significantly eroded the "public figure" versus "private figure" distinction.*

The *Gertz* Court, above all else, drew a sharp distinction between public figures and private figures. Public figures "have voluntarily exposed themselves to increased risk of injury from defamatory falsehood concerning them," unlike private figures. Moreover, "[p]rivate individuals are not only more vulnerable to injury than public officials and public

---

same size readership of the allegedly defamatory publication; such an inquiry would effectively prohibit widely read publications from ever commenting on local controversies. Our inquiry is rather whether the evidence demonstrates that the defamation plaintiff had access to channels of effective communication to respond to the allegedly defamatory statements. Carr clearly had such access.").

43. Media Matters has prepared a very thorough timeline of the Shirley Sherrod controversy. See *Timeline of Breitbart's Sherrod Smear*, MEDIA MATTERS (July 22, 2010, 7:38 AM), <http://mediamatters.org/research/201007220004>. Sherrod has sued Breitbart for defamation. See Ashley Hayes, *Former USDA Employee Sues Conservative Blogger Over Video Posting*, CNN POLITICS (Feb. 15, 2011, 11:15 AM), <http://www.cnn.com/2011/POLITICS/02/14/sherrod.lawsuit>. In her complaint she notably claims Breitbart acted with "actual malice." Complaint at 18, *Sherrod v. Breitbart*, No. 0001157-11 (Super. Ct. D.C. Feb. 11, 2011), available at <http://static1.firedoglake.com/28/files/2011/02/20110211-Sherrod-Complaint-File-Stamp.pdf>.

figures; they are also more deserving of recovery.” The *Rosenbloom* plurality opinion, by Justice Brennan, expressed a very different view: “Voluntarily or not, we are all ‘public’ men to some degree.”

Justice Brennan’s words ring even more true in the digital age. First, what the *Gertz* framework may have once offered in clarity or ease of administration no longer makes up for what it sacrifices in terms of accuracy. In the age of “microcelebrity,” fame—along with its associated benefits and burdens<sup>44</sup>—is distributed along a spectrum, not according to a dichotomy.<sup>45</sup> One way of thinking about this is through Chris Anderson’s “long tail” rubric.<sup>46</sup> Instead of a world with a few huge celebrities and millions of “nobodies,” we now live in a world with a “long tail” of minor celebrities (e.g., reality TV stars, prominent bloggers). As Anderson notes, “not all celebrities are Hollywood stars. As our culture fragments into a million tiny microcultures, we are experiencing a corresponding rise of microcelebrities.”<sup>47</sup>

Second, and on a closely related note, the *Gertz* approach fails to take into account the rise of “niche celebrity.” Thanks to the rise of highly targeted blogs, interest groups within social networks, or even social networking sites for specific interest groups, becoming a “celebrity” within a particular area of interest, trade or profession, or geographical location is startlingly easy.

A good example of a niche celebrity, related to the blog that one of us founded, Above the Law ([www.abovethelaw.com](http://www.abovethelaw.com)), might be Evan Chesler. Chesler is the presiding partner of Cravath, Swaine & Moore, one of the nation’s most powerful and prestigious law firms.<sup>48</sup> Chesler is

44. There’s a reason why people try out by the thousands for reality shows (i.e., the chance to be humiliated on national television). Fame has its privileges. See *Waldbaum v. Fairchild Publ’ns*, 627 F.2d 1287, 1294-95 (D.C. Cir. 1980) (“Fame often brings power, money, respect, adulation, and self-gratification. It also may bring close scrutiny that can lead to adverse as well as favorable comment. When someone steps into the public spotlight, or when he remains there once cast into it, he must take the bad with the good.”).

45. See Thompson, *supra* note 2 (“Microcelebrity is the phenomenon of being extremely well known not to millions but to a small group – a thousand people, or maybe only a few dozen.”); Sorgatz, *supra* note 2 (“The point is that renown is no longer the exclusive province of a select few. Nano-celebrity is there for the taking, if you really want it.”); Jason Tanz, *Internet Famous: Julia Allison and the Secrets of Self-Promotion*, WIRED, July 15, 2008 (noting that blogger Julia Allison “may not be famous by the traditional definition,” but that “to a devoted niche of online fans – and an even more devoted niche of detractors – she is a bona fide celebrity”).

46. CHRIS ANDERSON, *THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE* (2006).

47. *Id.*; see also Nicholas Lemann, *Amateur Hour*, THE NEW YORKER, Aug. 7, 2006, at 44 (“Most citizen journalism reaches very small and specialized audiences and is proudly minor in its concerns. David Weinberger, another advocate of new-media journalism, has summarized the situation with a witty play on Andy Warhol’s maxim: ‘On the Web, everyone will be famous to fifteen people.’”).

48. *Evan R. Chesler*, CRAVATH, SWAINE & MOORE L.L.P.,

not a public official, and he is not, by the traditional analysis, a general-purpose public figure. It would even be difficult to cast him as a limited-purpose public figure, since he is generally not trying to influence the resolution of any issue of public concern.<sup>49</sup> Chesler's decisions in leading Cravath are just decisions he makes in the course of doing his job—like the attorney in *Gertz*.

But Evan Chesler is, within the legal profession and the world of large law firms, a definite niche celebrity, a figure of great interest in this particular field. How should he be covered? The legal profession is wealthy, powerful, and prominent, and he is a leading figure within it. Why shouldn't he have to demonstrate "actual malice" with respect to reporting that covers his leadership of Cravath?

There are hints in prior case law that fame within a community or a sector can be constitutionally significant. As stated by the Court in *Rosenblatt v. Baer*, "[t]he subject matter may have been only of local interest, but at least here, where publication was addressed primarily to the interested community, that fact is constitutionally irrelevant."<sup>50</sup>

Niche celebrity might also be relevant in terms of evaluating the damage inflicted by falsehoods, a consideration identified by the *Gertz* Court in establishing greater protection for private individuals. The Supreme Court's major defamation precedents often involved plaintiffs with local or limited fame who were covered by giant news outlets with national or international reach, like the *New York Times* or *Time* magazine. Damages in such cases could be high, as at least one court has noted:

Dissemination to a wide audience creates special problems. For example, an individual may be well known in a small community, but the publication covers a larger area. In such a situation, it might be

---

<http://www.cravath.com/echesler> (last visited Apr. 1, 2011).

49. A possible exception to this might be the use of the billable hour as the dominant billing method for lawyers, if one considers this to be an issue of public concern. Chesler has mounted a vigorous critique of the billable hour, speaking out and writing against it in widely read, mainstream-media publications. *E.g.*, Evan Chesler, *Kill the Billable Hour*, FORBES, Jan. 12, 2009, at 26.

50. *Rosenblatt v. Baer* 383 U.S. 75, 83 (1966); *see also* *Lorain Journal Co. v. Milkovich*, 474 U.S. 953, 963 (1985) (Brennan, J., dissenting from denial of certiorari) (arguing that a high school wrestling coach was a limited purpose public figure because of his involvement in "a public controversy of concern to residents of the local community [that was] as important to them as larger events are to the Nation"); *id.* at 964-65 (arguing that the Court's commitment to free speech "applies as much to debate in the local media about local issues as it does to debate in the national media over national issues," and that "[t]his Court's obligation to preserve the precious freedoms established in the First Amendment is every bit as strong in the context of a local paper's report of an incident at a local high school as it is in the context of an advertisement in one of the Nation's largest newspapers supporting the struggle for racial freedom in the South").

appropriate to treat the plaintiff as a public figure for the segment of the audience to which he is well known and as a private individual for the rest. In any event, the defamation's audience may be relevant in assessing damages, for injury may be less if the audience does not know of the victim and will have no occasion to interact with him in the future.<sup>51</sup>

Of course, this gives rise to another question: Why are niche publishers—who might cover matters that are important to just a limited group of people, or even matters of debatable importance—entitled to full First Amendment protection? The response can be found in the Supreme Court's decision in *Time, Inc. v. Hill*, which takes a commendably broad view of free speech:

The guarantees for speech and press are not the preserve of political expression or comment upon public affairs, essential as those are to healthy government. One need only pick up any newspaper or magazine to comprehend the vast range of published matter which exposes persons to public view, both private citizens and public officials. . . .

Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period. No suggestion can be found in the Constitution that the freedom there guaranteed for speech and the press bears an inverse ratio to the timeliness and importance of the ideas seeking expression.<sup>52</sup>

One might argue that providing niche publishers with broad constitutional protection fails to consider Google and other search engines, which effectively take what might have been a niche publication, read by a limited audience, and broadcast it to a much wider range of readers. But using one of these search engines already places the user in “niche” territory. Unlike the front page of the *New York Times* or another general-interest newspaper, where a reader might come across a defamatory falsehood about someone the reader had never heard about before and had no prior interest in, a search engine isn't putting in front of the user information that the user wasn't already looking for in a targeted way.

Finally, technology has eroded privacy in so many different ways. As Justice Brennan declared in *Rosenbloom*, “[v]oluntarily or not, we are all ‘public’ men to some degree.” Or as Justice Brennan wrote in the earlier

---

51. *Waldbaum v. Fairchild Publ'ns*, 627 F.2d 1287, 1295 n.22 (D.C. Cir. 1980).

52. *Time, Inc. v. Hill*, 385 U.S. 374, 388 (1967) (internal citations omitted).

case of *Time, Inc. v. Hill*:

Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press.<sup>53</sup>

In this day and age—of blogs, where our private misadventures can be written about at length; of streaming video and YouTube, where said misadventures can be seen and heard by total strangers; of Facebook, where “friends” can post pictures of us, against our will (maybe we can “de-tag,” but we can’t remove); of full-body scanners at the airport—Justice Brennan’s words ring more true than ever, for better or worse. We are more “public” and more interconnected than ever.

Of course, one could imagine a regime in which people who went out of their way to protect their privacy—e.g., Howard Hughes-like hermits, who eschew Facebook and Twitter, don’t leave home often, etc.—might be treated differently under the law, and given more favorable treatment as defamation or privacy-tort plaintiffs. But the default rule—for average people, who take no extraordinary measures to protect her privacy—would treat them as fairly public individuals.

C. *Objections to adoption of the Rosenbloom rule can be overcome.*

The most obvious counterargument is that adopting the *Rosenbloom* rule and applying the “actual malice” standard even to private individuals, as long as the subject matter is of public or general concern, would create a regime too favorable to publishers, speakers, and defamatory speech at the expense of private citizens. There are several responses to this position.

First, the experiences of various states suggest that *Rosenbloom* is a workable standard. At least three states, Colorado, Alaska, and Indiana, have essentially adopted the *Rosenbloom* approach, and two others, New Jersey and New York, have standards similar to *Rosenbloom*.<sup>54</sup> There is no indication that the *Rosenbloom* rule has proven unworkable or resulted in excessive defamatory speech in these jurisdictions.

Second, to the extent that *Rosenbloom* results in a more favorable regime for publishers and speakers, it simply reflects the law evolving to

53. *Id.*

54. James C. Mitchell, *Rosenbloom’s Ghost: How a Discredited Decision Lives on in Libel Law*, 40 IDAHO L. REV. 427, 436–38 (2004). Mitchell’s main criticism of *Rosenbloom* is that deciding what constitutes a matter of “public concern” can be difficult—a subject that lies beyond the scope of the current discussion, but certainly an important issue for courts that follow *Rosenbloom* to keep in mind.

accommodate advances in communications technology. Free speech and First Amendment concerns receive strong legal protection in the online context—perhaps most notably thanks to Section 230 of the Communications Decency Act of 1996, which insulates operators of interactive computer services from being held liable for defamatory content provided by third parties.<sup>55</sup> As the Ninth Circuit stated in *Batzel v. Smith*, construing Section 230:

Congress made this legislative choice [of enacting Section 230] for two primary reasons. First, Congress wanted to encourage the unfettered and unregulated development of free speech on the Internet, and to promote the development of e-commerce. Section 230(a), “Findings,” highlights that:

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.<sup>56</sup>

Applying old rules to new media does not make sense as a policy matter. It would prevent society from reaping the full rewards of new communications technologies by inhibiting speech. As the Fourth Circuit explained in *Zeran*:

Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect.<sup>57</sup>

Accordingly, by enacting Section 230, Congress replaced the traditional tort law doctrine of republication liability with a new framework for the online world. It’s a compromise that seems to have worked fairly well; almost 15 years after its enactment, Section 230 is alive and well.

Finally, adoption of the *Rosenbloom* rule is not the most extreme pro-media/pro-free-speech position one could take. Justices writing decades ago articulated stronger viewpoints. For example, Justices Black

55. 47 U.S.C. § 230 (1998).

56. *Batzel v. Smith*, 333 F.3d 1018, 1027 (9th Cir. 2003); *see also Zeran v. America Online, Inc.*, 129 F.3d 327, 330-31 (4th Cir. 1997) (“The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.”).

57. *Zeran*, 129 F.3d at 331 (citations omitted).

and Douglas expressed the view that even the *New York Times* standard infringes on free speech unconstitutionally—despite the fact that it is a standard that makes it very difficult for libel plaintiffs to prevail.<sup>58</sup>

## CONCLUSION

Justice Brennan's observation that "we are all 'public' men to some degree," from a 1971 opinion, has proven prescient. Some 35 years later, writers in the Internet age would observe that "[w]e are all public figures now."<sup>59</sup> The legal understanding of who is a public figure must now catch up.

On a somewhat optimistic note, there are some indications that libel lawsuits are decreasing—perhaps as a result of some of the changes in the media landscape discussed above. It appears that the number of libel cases going to trial has declined:

The number of libel cases going to trial has dropped to the point where it's not worth doing the survey on an annual basis, said Sandy Baron, the executive director of the Media Law Resource Center. Ms. Baron was speaking about the annual-and now biannual-survey of libel and privacy trials that her firm rounds up and produces into a study. In the most recent study, the Media Law Resource Center found that libel trials in the 2000s were down more than 50 percent from the 1980s. In the 1980s, the center found 266 trials; in the '90s, that number dropped to 192; in the past decade it dropped to 124. In 2009, only nine surfaced.<sup>60</sup>

What's behind the change? Perhaps the Web, which has (1) created a flood of content, making any individual negative publication less prominent, and (2) given aggrieved parties more outlets for responding to criticism they see as unfair.<sup>61</sup>

---

58. *See, e.g.*, *New York Times Co. v. Sullivan*, 376 U.S. 254, 293 (1964) (Black, J., concurring) (explaining that "I vote to reverse exclusively on the ground that the Times and the individual defendants had an absolute, unconditional constitutional right to publish in the Times advertisement their criticisms of the Montgomery agencies and officials"); *Time, Inc.*, 385 U.S. at 374, 398 (1967) (Black, J., concurring) (predicting that the *New York Times* "doctrine too is bound to pass away as its application to new cases proves its inadequacy to protect freedom of the press"); *id.* at 401 (Douglas, J., concurring); *Gertz v. Robert Welch, Inc.*, 418 U.S. 334, 356 (1974) (Douglas, J., dissenting) ("I have stated before my view that the First Amendment would bar Congress from passing any libel law.").

59. David Lat, *Brokeback Lawfirm: Gera Grinberg — Who Is This Guy?*, ABOVE THE LAW (Feb. 14, 2007, 1:52 PM), <http://abovethelaw.com/2007/02/brokeback-lawfirm-gera-grinberg-who-is-this-guy/>; Tanz, *supra* note 45.

60. John Koblin, *The End of Libel*, THE NEW YORK OBSERVER MEDIA MOB (June 8, 2010, 9:23 PM), <http://www.observer.com/2010/media/end-libel>.

61. *Id.* (citing a media lawyer who stated, "[p]eople who used to feel frustrated that they couldn't get their viewpoint across now can" by "put[ting] their response on a Web site" or "find[ing] an outlet that will publish it").

It is too early to know, however, whether the recent decline in libel trials will be a lasting development. Rather than assume this to be the case, society is far better served by recognizing and revisiting the archaic legal precedent surrounding modern defamation law. Only by rejecting *Gertz* and adopting Justice Brennan's more fluid *Rosenbloom* position, treating us all as public figures to some degree, can such law begin to make sense in the age of new media and social networks.



# FIRST-CLASS OBJECTS

JAMES GRIMMELMANN\*

“You are not special. You are not a beautiful or unique snowflake.”<sup>1</sup>

|     |  |     |
|-----|--|-----|
| I.  | UNIQUE IDENTIFIERS.....                            | 421 |
|     | <i>A. James Grimmelmann and @grimmelmann</i> ..... | 422 |
|     | <i>B. Unique Identifiers</i> .....                 | 424 |
|     | <i>C. Other Examples</i> .....                     | 426 |
| II. | CONSEQUENCES.....                                  | 427 |
|     | <i>A. Standardization</i> .....                    | 427 |
|     | <i>B. Third Parties</i> .....                      | 429 |
|     | <i>C. Knowledge Creation</i> .....                 | 430 |
|     | <i>D. Representation</i> .....                     | 431 |
|     | <i>E. Control</i> .....                            | 433 |
|     | CONCLUSION.....                                    | 434 |

## I. UNIQUE IDENTIFIERS

How should we think about privacy in a digital age? One approach is to focus on how people use computers: how what we choose to share about ourselves changes when we go online.<sup>2</sup> But we could also focus on how computers use people: how flows of personal information are transformed by technology. Just as e-mail is different from mail, a spycam is different from a spy.

This brief essay will examine a seemingly technical question: *how are people represented within computer systems?* The essay will argue that there are two possible ways to do it, and that the choice between them has important technical, social, and humanistic consequences. It won't

---

\* Associate Professor of Law, New York Law School. I presented earlier versions of this paper at the Privacy and Innovation Symposium at Yale Law School and the Privacy and the Press conference at the University of Colorado Law School. My thanks for their comments to the attendees there, to the participants in the MSRNE Social Media Collective mailing list, and to Aislinn Black, Frank Pasquale, and Tal Zarsky. This essay is available for reuse under the Creative Commons Attribution 3.0 United States license, <http://creativecommons.org/licenses/by/3.0/us>.

1. Fight Club (Fox 1999).

2. See, e.g., James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1147-50 (2009).

say much new about those consequences—instead, it will show how closely linked they are.

*A. James Grimmelm and @grimmelm*

The difference is illustrated by a tweet. On October 27, Ryan Calo sent the following text to Twitter:

Privacy and innovation thought pieces by Helen Nissenbaum, Frank Pasquale, @grimmelm, and others up on Yale ISP.  
<http://bit.ly/aUtk0v3>

Let's examine two parts of this tweet: "Frank Pasquale" and "@grimmelm".<sup>4</sup> Syntactically, they're both strings of characters from the Latin alphabet, enriched with some standard punctuation symbols. They contain 14 and 9 characters, respectively. In the standard UTF-8 encoding used by Twitter,<sup>5</sup> they would take up 14 and 9 bytes, that is, 112 and 72 individual ones and zeros.<sup>6</sup>

Semantically, "Frank Pasquale" and "@grimmelm" are both names; their preferred interpretation is that they refer to people. "Frank Pasquale" is what Calo typed so that readers of his tweet would know he was talking about Frank Pasquale, the Schering-Plough Professor in Health Care Regulation and Enforcement at Seton Hall Law School. "@grimmelm" is what Calo typed so that readers would know he was talking about me.

This second meaning requires some explanation. "grimmelm" is my Twitter username, so "@grimmelm" is a way of referring to me. Since Twitter limits all posts to 140 characters, space is at a premium, and concision is essential. In 2007, Twitter user Chris Messina started using the pound symbol "#" to flag the topics of his tweets, such as "#barcamp" for a message of interest to attendees of the Bar Camp event.<sup>7</sup> These "hashtags" caught on, and millions of Twitter users began deploying them to annotate a wide range of tweets. The Twitter community embraced other compressed forms, such as the dollar sign "\$" followed by

3. Ryan Calo, TWITTER (Oct. 27, 2010, 12:24 AM), <http://twitter.com/#!/rcalo/status/28913525284>.

4. Here, and throughout this essay, I have moved punctuation marks outside of quotations for purposes of precision.

5. See *Counting Characters*, TWITTER DEVELOPERS, [http://dev.twitter.com/pages/counting\\_characters](http://dev.twitter.com/pages/counting_characters) (last visited Feb. 24, 2011).

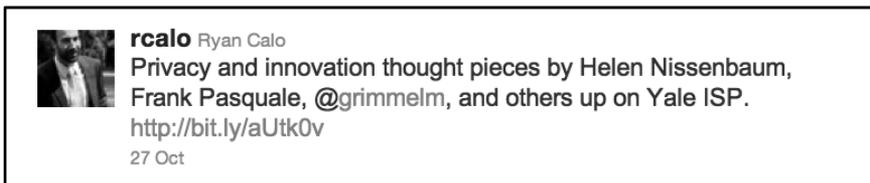
6. See UNICODE CONSORTIUM, *THE UNICODE STANDARD 3-5* (5th ed. 2006); JUKKA K. KORPELA, *UNICODE EXPLAINED 298-300* (2006).

7. See Chris Messina, *Groups for Twitter; or A Proposal for Twitter Tag Channels*, FACTORYCITY (Aug. 25, 2007, 10:00 PM), <http://factoryjoe.com/blog/2007/08/25/groups-for-twitter-or-a-proposal-for-twitter-tag-channels>.

a stock ticker symbol to refer to a company (e.g., “\$”<sup>8</sup>), and the at-sign (“@”) followed by a username to refer to a particular user (e.g., “@grimmelm”).<sup>9</sup>

Within the community of Twitter users, “James Grimmelm” and “@grimmelm” would both be recognized as valid names for me. A Twitter user who knew me would understand that they referred to me; a Twitter user who didn’t know me would still surmise that they referred to someone with that name or username. These usages are both conventional. True, the tradition of assigning and capitalizing names is older, more widely known, and more universally followed. More people will recognize “James Grimmelm” than “@grimmelm”. But at root, they are both conventions within an interpretive community of humans.

Twitter, however, treats “Frank Pasquale” and “@grimmelm” differently. Here is what Calo’s tweet looked like on Twitter’s website:



In the posted version, “Frank Pasquale” appears normally, in black type. “grimmelm”, however, appears in red. That’s because it’s a hyperlink; it links to my profile page on Twitter. Once the @-syntax caught on among users, Twitter adapted to it. The company reprogrammed its software to turn each such string—an “@” followed by a username—into a hyperlink to that user’s profile page on Twitter.com.<sup>10</sup>

This isn’t just a difference between one kind of name and another—“James Grimmelm” versus “@grimmelm”. It also means that Twitter can make distinctions among users who are named in tweets. Old-school plain-text names, such as “James Grimmelm” and “Ryan Calo”, are blobs of unstructured data, no different from “d#fh@3.pQMNa0”. But tweets with “@rcalo” and “@grimmelm” and “@amturing” now have structure; Twitter’s software can and does do different things depending on who is named by the tweet. For example, Twitter now builds for each

8. *See, e.g.*, Mad Money on CNBC, TWITTER (Feb. 3 2010, 6:11 PM), <http://twitter.com/#!/MadMoneyOnCNBC/status/33346776282963969>.

9. *See, e.g.*, David Christiansen, *How to Use @Reply in Twitter Messages*, INFORMATION TECHNOLOGY DARK SIDE (Mar. 11, 2009), <http://www.techdarkside.com/how-to-use-reply-in-twitter-messages>.

10. @Ev [Evan Williams], *How @Replies Work on Twitter (and How They Might)*, TWITTER BLOG (May 12, 2008, 10:51 AM), <http://blog.twitter.com/2008/05/how-replies-work-on-twitter-and-how.html>.

user a list of the tweets that mention her, whoever they were posted by.<sup>11</sup>

### B. *Unique Identifiers*

Twitter's user database is central to its ability to make "@grimmelm" meaningful. If I write "@asdfasdfhjsa" in a tweet and click on the link that results, Twitter will display an error message that says, "This user does not exist." Twitter has a list which records the facts that "grimmelm" and "rcalo" are usernames but that "d#fh@@3.pQMNa0" and "asdfasdfhjsa" are not. In particular, Twitter's database assigns a *unique identifier* to each user. Since unique identifiers are ubiquitous in computer science, it will be helpful to discuss the technical considerations behind them.

Unique identifiers come from the world of databases, in which one seeks to store information about the world in a structured manner.<sup>12</sup> One way of thinking about the problem is that one wants to keep track of things and how they relate to each other. The widely-used "entity-relationship model" formalizes this idea by describing the world as a collection of *entities*.<sup>13</sup> "An entity is a 'thing' which can be distinctly identified. A specific person, company, or event is an example of an entity."<sup>14</sup> One describes the world by specifying the *attributes* that entities have (e.g., "John Doe's height is 5'9") and the *relationships* in which they participate (e.g., "John Doe and Jane Roe are married"). Unique identifiers pervade the model. Not only is an entity defined in terms of its ability to be uniquely identified, but to say that an entity has an attribute or participates in a relationship, one needs to be able to identify the entity in question.

Similar questions arise when one confronts the problem of database design: how best to store a representation of the world in a computer database. The dominant modern database paradigm is the "relational model," in which a database consists of a collection of *tables*.<sup>15</sup> The "table" metaphor is based on the two-dimensional display of tabular data on paper in rows and columns. Each row (or *entry*) consists of a series of

11. See *What Are @Replies and Mentions?*, TWITTER HELP CENTER, <http://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/14023-what-are-replies-and-mentions> (last visited Feb. 24, 2011).

12. See generally RAGHU RAMAKRISHNAN & JOHANNES GEHRKE, DATABASE MANAGEMENT SYSTEMS (2d ed. 1999); C.J. DATE, AN INTRODUCTION TO DATABASE SYSTEMS (7th ed. 1999); ABRAHAM SILBERSCHATZ ET AL., DATABASE SYSTEM CONCEPTS (6th ed. 2010).

13. See Peter Pin-Shan Chen, *The Entity-Relationship Model—Toward a Unified View of Data*, 1 ACM TRANSACTIONS ON DATABASE SYS. 9 (1976).

14. *Id.* at 10.

15. See E.F. Codd, *A Relational Model of Data for Large Shared Data Banks*, 13 COMM. ACM 377 (1970).

*values*, one each from the categories named by the column headings (or *fields*). For example, a course's table in a registrar's database might store the value "4" where the row for Wills and Trusts intersects the column for number of credits.<sup>16</sup> More concisely and precisely, we would say that the entry for Wills and Trusts has the value "4" in the number-of-credits field.

Here again, unique identifiers are pervasive. They are often necessary if we are to meaningfully combine, or *join*, the information from multiple tables.<sup>17</sup> Unless we have a way to know that the Wills and Trusts in the courses table is the same as the Wills and Trusts in the table of student schedules, there is no way to generate student transcripts with the correct number of credits. Giving Wills and Trusts a unique identifier—a common value that appears in both tables—provides an answer. A large literature on database design deals with the problem of finding or creating identifiers, or *keys*, that suffice to tell different rows apart, and with ensuring that their usage in different tables is consistent enough to permit meaningful joins.<sup>18</sup>

The vital role of unique identifiers for users in Twitter should now be apparent.<sup>19</sup> When a new tweet refers to me or to Ryan Calo using @-syntax, Twitter determines which user it should be associated with by consulting the database. Whenever any new information that should be connected up with a particular user comes in—a password change, a new tweet, a new follower, etc.—that information is added to another table in an entry that also includes that user's unique identifier. Everywhere inside Twitter's systems that a unique identifier goes, it is intended to refer to a specific user, and does.

Users are entries in Twitter's databases; they have unique identifiers. By contrast, for example, musical notes are *not* entries in Twitter's databases. Neither are cities, emotions, galaxies, cars, or judicial opinions. One can talk about these things on Twitter, and much much more, but not in a way that Twitter's servers will understand in the slightest. In contrast, one can talk about Twitter users in a way that Twitter will get; it will know *who* you're talking about, and be able to

16. The "intersection" is metaphorical, of course.

17. See, e.g., RAMAKRISHNAN & GEHRKE, *supra* note 12, at 97–98.

18. See, e.g., DATE, *supra* note 12, at 258–64.

19. Twitter does not use these character strings as the actual unique identifiers. Instead, because numbers are easier for computers to work with than strings, Twitter assigns each user a unique ID number. See, e.g., *Twitter REST API Method: users show*, TWITTER API DOCUMENTATION, <http://apiwiki.twitter.com/w/page/22554755/Twitter-REST-API-Method:-usersshow> (last visited Feb. 24, 2011). Whenever it sees a @username in a tweet, Twitter translates it into the appropriate ID number and uses the number internally from then on. Cf. *Find your Twitter ID*, IDFROMUSER.COM, <http://www.idfromuser.com> (last visited Feb. 24, 2011) (allowing one to look up the corresponding numerical user ID by typing in a Twitter user's screen name).

react accordingly. Unique identifiers are the essential catalyst in transforming messes of unstructured information into useful, structured data about people.

### C. *Other Examples*

This phenomenon is hardly confined to Twitter. Many other computer systems use unique identifiers for people. Consider a few more examples:

Facebook was designed from the ground up to give people unique identifiers. It assembles real names and other personal information into highly-structured profiles linked to a unique user identifier.<sup>20</sup> These profiles can be sorted, searched, and automatically manipulated. Try clicking on a favorite movie in a friend's profile, for example, and part of the resulting page will contain a list of your friends who also picked that movie as a favorite—a computation that joins multiple database tables (your friends, favorite movies) by matching unique identifiers. Facebook is thus profoundly oriented towards associating information with people: it collates, categorizes, analyzes, exposes, and projects them.

Another classic example of databases in which entries represent people is the credit reporting agency.<sup>21</sup> In order to report a credit history or credit score for a person, the agency must maintain a file for that person. This file takes the form of a unique identifier that is then cross-linked in a database with every transactional datum available on the person to whom that identifier corresponds: mortgage payments, credit card limits, past addresses, and much much more. Social Security numbers have traditionally been the unique identifier of choice, but due to fraud and mistakes, they're not always entirely reliable.

By way of contrast, consider the Wayback Machine's near-comprehensive archive of the Web.<sup>22</sup> It crawls the Web repeatedly, taking snapshots of every webpage it finds. Users can then retrieve a historical archive of any given webpage, seeing what it looked like on various dates stretching out across years. Many of these pages refer to people. When they do, however, the Internet Archive has no idea that they do. Names are just blobs of text, indistinguishable from any of the other blobs of text in the archived webpages. People are *not* entries in the Internet Archive's databases.<sup>23</sup>

---

20. See, e.g., Grimmelmann, *supra* note 2.

21. See, e.g., Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1408 (2001).

22. INTERNET ARCHIVE WAYBACK MACHINE, <http://waybackmachine.org> (last visited Feb. 24, 2011).

23. If I retrieved pages from the Wayback Machine and then scanned them for text that looked likely to be a name, I might create a system that had identifiers for people, but the

## II. CONSEQUENCES

Let us explore some of the consequences of giving people unique identifiers in order to create database entries on them. This simple technical move has surprisingly wide-ranging effects. It connects to so many observations in privacy and technology scholarship that it suggests there is something fundamental about the shift. Unique identifiers are the key, so to speak, to the process by which computer systems become *about* people.

### A. Standardization

Unique identifiers and structured data are inherently *standardized*. By imposing structure, one can produce a well-defined representation that is free from much of the ambiguity of unstructured data. As we shall see, this standardization is central to the tremendous power of unique identifiers. But since the world is itself unstructured and ambiguous, the process of standardizing identifiers introduces its own errors. I will break standardization down into four components: *uniqueness* of identifiers, *normalization* of them to give people canonical names, the inevitable *errors* that result, and the discontinuous way in which data attached to unique identifiers *decays*.

Ordinary names aren't unique: think of "John Smith".<sup>24</sup> Compare that with Twitter usernames: there is only one "@grimmelm". The "unique" in "unique identifier" requires that different people have different identifiers. The flipside of uniqueness is normalization. Sometimes people call me "Jim", which isn't quite right—but isn't quite wrong, either. These slippages are unproblematic in everyday life, but the kind of contextual insights people bring to the table are hard for computers to replicate. Unique identifiers deal with the problem by making identifiers canonical. Instead of dithering over whether I prefer to be called "James" or "Jim", just use "@grimmelm". It does the right thing.

Getting to @grimmelm, however, isn't as easy as it looks. The first problem is inherent in the need for uniqueness: the real world is filled with people who use identical or confusingly similar names. Precisely because there can be only one "@grimmelm", only one of us can have it, and that means conflict. The endemic and enduring fights over domain names<sup>25</sup> are echoed in the land-rush every time a new social media service

---

process would be imperfect, approximate, and error-prone.

24. See James Gleick, *Get Out of My Namespace*, N.Y. TIMES MAG., Mar. 21, 2004, at 44 ("You don't own your name. Just ask any John Smith.").

25. See generally JACQUELINE LIPTON, INTERNET DOMAIN NAMES, TRADEMARKS, AND FREE SPEECH (2010).

hands out identities on a first-come, first-served basis.<sup>26</sup> Even using artificial identifiers can be a technical challenge: they need non-trivial infrastructure to create, distribute, and manage.<sup>27</sup> Name assignment is inherently political.<sup>28</sup>

The second problem is that while a set of unique identifiers may be clean and well-structured, the world is anything but. The process of mapping the world onto those identifiers can never be specified completely and correctly. Someone has to enter the data; that someone will make typos and bad guesses. Whenever data from two different databases or sources is to be combined (which is quite often, as unique identifiers make this aggregation attractive), mismatches between their identifiers introduce fresh errors. Identity theft, wrong addresses, conflation with other people with the same name—all of these crossed wires can be triggered when a credit file is populated with outside information which is mistakenly assigned to your identifier in the database. In database terminology, these mistakes are the results of an improperly specified join operation—one that combines two tables using a poorly-chosen key.

Another source of error is the passage of time, and here, structured data is a mixed blessing. On the one hand, standardization plays a centripetal role by facilitating error correction. Misspellings and other minor mistakes are easier to spot and repair before they cascade and feed each other. On the other hand, digitization and centralization increase the risk of truly catastrophic failure. For example, when the servers supporting Microsoft's Sidekick mobile phone customers failed, thousands of users suddenly lost access to their contact books.<sup>29</sup> The price we pay for resilience against daily small errors is a greater risk of a single big failure.

Standardization helps here: many or most random errors become easily-spotted syntactic mistakes (think of how much faster it is to spell-check a word processing document than the same manuscript in printed form). Normalization plays a centripetal role, fixing up misspellings and eliminating other minor mistakes before they multiply and feed each other. On the other hand, this centralization increases the risk of truly catastrophic failure.

---

26. See, e.g., Verne Kopytoff, *Facebook Land Rush to Start in Three Days*, TECH CHRON. (June 9, 2009, 3:45 PM), [http://www.sfgate.com/cgi-bin/blogs/techchron/detail?entry\\_id=41455](http://www.sfgate.com/cgi-bin/blogs/techchron/detail?entry_id=41455).

27. See, e.g., INT'L TELECOMMS. UNION, STANDARD X.667 (2004) (34-page international standard on generating and distributing unique identifiers).

28. See generally MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 87-88 (2004).

29. See Rob Pegoraro, *Sidekick Users See Their Data Vanish Into a Cloud*, WASH. POST, Oct. 13, 2009, at A14. Sidekick users' information, such as address books and to-do-lists, was primarily stored on company servers. Maintenance of the servers went wrong, and backups proved unusable, locking users out from their data.

## B. *Third Parties*

Unique identifiers don't just happen on their own. Someone has to build the database, create identifiers, and ensure that they really are unique. The use of unique identifiers, in other words, is inherently tied to particular *third parties*. “@grimmelm” has its special meaning because of Twitter's efforts. Similarly, you need to consult a credit agency's files to run a credit report on someone, and social security numbers depend on the Social Security Administration's coordinating role. Without these third parties, unique identifiers lose their special meanings. If Twitter vanished tomorrow, “@grimmelm” would become an ordinary name again, like “James Grimmelm”. People could still use it to refer to me, but this would be a matter of convention and tacit human knowledge, not an automated, fixed reference.

We will have much more to say about third parties, but for the moment, I would like to emphasize two ways in which their special role manifests itself: the *dependence* users have on the third party's continued support, and the *lock-in* the third party enjoys against user attempts to switch to another third party. Dependence first: The more valuable and important an identifier, the more one has to lose if it goes away. Because a unique identifier is controlled by a specific entity, rather than being dispersed throughout a community, as a traditional name would be, one becomes dependent on the entity. The third party who holds a unique identifier holds the name itself hostage, and possibly the person. As anyone who's been locked out of their e-mail account can attest, losing an important unique identifier can be devastating. If Facebook collapses, all the information locked in its proprietary formats and adapted to its social network will be simply gone.

These third parties also enjoy a kind of lock-in effect, precisely because *other people* use them to interact with and learn about you. No one wants to be the only person on a social network; no one would query a credit agency with a single file. But if everyone in your industry is on LinkedIn, you may need to be too, and if every landlord uses the same background-check service, you had better worry about what your file says about you.

Compounding the problem, it's much harder to move structured data around than unstructured data. To leave Facebook for a competing social network, for example, I will need to export the data in a structured format (which Facebook does not currently allow or enable), and find a competitor using a compatible format for its own data.<sup>30</sup> Then there is

---

30. See Robert Scoble, *Facebook Has a Point Where It Comes to Your Privacy*, SCOBLEIZER (May 15, 2008), <http://scobleizer.com/2008/05/15/facebook-has-a-point-where-it-comes-to-your-privacy>.

the problem of interoperability: for example, Facebook now provides login services for other websites and services, including Skype. One could see this either as making identity more portable by allowing a user to sign in only to Facebook, or as making identity less portable by forcing everything to flow through Facebook.

### C. *Knowledge Creation*

Using unique identifiers for people enables a wide variety of practices that involve the *creation of knowledge* about them. I will bring out four, which build on each other: the *aggregation* of information about a person from multiple sources, *automated reasoning* about a person from multiple pieces of information, the *enumeration* of all of the references to a given person in a database, and *statistical analysis* about populations by summarizing information about multiple people.

Unique identifiers are remarkably convenient focal points for data aggregation. Within a database, this is often the point of having unique identifiers at all: to allow them to serve as keys for joining data from two different tables. That works with unique identifiers; it doesn't work without them. The registrar can put information about my courses from the courses table together with information about me from the faculty table to produce a personalized schedule that indicates when I am expected to be in class. There is more information in this combined view than there was in either table alone. This same phenomenon can happen on a larger scale when multiple databases are brought together—or when new information is added to an existing database. Having entries for people in a database is an essential step in bringing together information about them from many different sources.

Once multiple pieces of information are associated with a person in a database, it becomes possible to ask a computer program to engage in automated reasoning about them. A credit score is one kind of automated reasoning: one that results from algorithmically combining large quantities of financial data according to a set formula. Similarly, Foursquare can conclude that multiple people are in the same physical space based on their separate check-ins, and Amazon can recommend new books based on previous ones you've purchased, viewed, and reviewed. This is the Semantic Web dream, of course: everything encoded in a way that supports the creation of complex relationships of out simpler pieces—that is, drawing conclusions on the basis of aggregated data.<sup>31</sup>

One particularly simple, but important, form of automated reasoning is *enumeration*: listing all of the references to a given person.

---

31. See Tim Berners-Lee et al., *The Semantic Web*, SCI. AM., May 2001, at 34, 36-38.

That is, you can look through Twitter for all the tweets that mention a user or through Facebook for all the photos in which someone is tagged, and have high confidence that you have seen all such items that are possible for you to see. This property depends on normalization and the use of third parties. The third party is a single source maintaining a complete list of data about a person, and normalization means there is a standard way of ensuring that all references to that person are associated with their digital identifier. This property doesn't hold in general; I am quite certain that I don't know all of the places I'm referenced on the Web. For a lawyer doing due diligence, a private investigator building a file, or a nervous college student untagging photos of herself at a keg party, enumeration is a godsend.

A different way to extend automated reasoning is to draw conclusions not about individuals but about populations. This is the goal of statistical reasoning. Here, the use of unique identifiers reaches back far beyond the dawn of digital computing, into the parallel growth of bureaucracy and demography. The data miner deciding which customers are most likely to respond to a promotional flyer for a new toothpaste, the transportation planner estimating the number of subway cars needed over the next five fiscal years, and the pollster gauging support for a candidate are all dealing with abstracted statements about people. The unique identifiers may have receded into the background here, but note that these exercises are futile unless they start by identifying and differentiating the characteristics of individuals. Gauging the likely outcome of an election by surveying the same person five hundred times is ridiculous; surveying five hundred different people is not.

#### D. Representation

We have noted that unique identifiers are essential for representing people in databases. But there is another kind of *representation* that they enable: to other people. Unique identifiers are pervasively linked to social uses of digital technology, because they play all sorts of roles in shaping the presentations of people that other people see. I would like to call out four in particular: voluntary *self-presentation* by shaping how one's digital persona is built up, increased and involuntary *visibility* of one's actions and attributes, the possibility of *misrepresentation* of a person by a distorted digital persona, and proactive *monitoring* of one's digital presence.

How does an online persona differ from the numerous offline personas people have always created for particular social roles? A unique identifier provides a centralizing, coordinating location for aggregating various personal qualities into the digital self one wishes to show to the world: an e-mail address or a social network profile. Beyond that,

though, people seem almost to gravitate to using structured data for their self-identification. From the Geek Code to the well-defined slots in a Facebook profile to the millions of online quizzes people fill out to tell others about themselves,<sup>32</sup> there seems to be a natural enthusiasm for crafting digital avatars using well-defined categories.<sup>33</sup> It may have to do with the creativity-promoting qualities of constraint, but also with the social usefulness of structured signals. A unique identifier provides the fixed point to which these additional attributes can be attached in a structured way.

On the other hand, if you're in a database, it's harder to hide. You're more visible, because data sticks to unique identifiers like cat hair to sweaters. We all know about the gigantic databases that commercial profilers have on all of us. These identifiers also help stalkers and other private individuals do the same. If I'm trying to look you up, I can get much further once I figure out what your Twitter handle is. You may not have put your real name on the account, but if I can infer that it's you, the centralized, normalized role that it plays helps me build an extensive file on you quickly. It is no accident that thinkers have cast about for metaphors to express the uniquely personal, uniquely threatening characteristics of these new databases: Daniel Solove's "digital dossiers,"<sup>34</sup> John Battelle's "database of intentions,"<sup>35</sup> Paul Ohm's "databases of ruin."<sup>36</sup>

Moreover, visible data need not be correct data; we have already noted the pervasiveness of errors in databases about people. Not only can anyone who supplies data about a person get it wrong, but the third parties who control the unique identifiers have a special kind of power over how a person is represented. Just as a credit rating agency can destroy my ability to get a mortgage, Facebook could metaphorically scribble a mustache on my profile or Twitter could redirect every mention of "@grimmelm" to my mortal enemy.

With enumeration, however, comes the possibility that one could protect one's privacy through proactive monitoring. If you want to keep something secret, but there are many places where people could be talking about the secret, then you have a Pokemon problem: gotta catch 'em all. It is much easier for you to make that search when you can

32. See, e.g., Which Hegel's Phenomenology of Spirit Character Are You? SELECTSMART.COM, (October 2000), <http://www.selectsmart.com/FREE/select.php?client=hupitesti>.

33. See Grimmelmann, *supra* note 2, at 1176.

34. DANIEL SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 2* (2006).

35. JOHN BATTELLE, *THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE* 1-2 (2005).

36. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 (2010).

enumerate *every* reference to yourself. Facebook, for example, sends me a message every time someone tags a photo of me, and lets me refuse entirely to be tagged in Places.<sup>37</sup> This works only imperfectly in a non-centralized, non-normalized space like the Web. It leaves me dependent, however, on the good will of the third party to let me step through all of the relevant references. If it hides the references from me, I can do nothing.

### E. Control

Finally and most famously, unique identifiers profoundly shape the dynamics of power and *control* around personal information. Some of these moves empower individuals; others leave them comparatively helpless. I will bring out four themes from these extensive debates, all of which can be linked to unique identifiers: *empowerment* of individuals by helping them accumulate self-knowledge in a structured way, *panoptic control* of individuals by outside entities who use the identifier as a focal point, *manipulation* of individuals by those who use detailed personal profiles to shape what they see and think, and the pure existential *objectification* of individuals by others who “reduce” them to an entry in a database.

Start with empowerment: Having structured data about oneself in digital form can be useful. The electronic health record is probably the best example. It’s enormously helpful for me to have a single digital file that I can share with a new doctor, rather than there being scattered information about me in different locations, digital and paper, which I have to search out, pore through, and compile. This is the positive face of aggregation. Lifelogging is a kind of self-help version of aggregation with precisely this goal: collecting and collating large quantities of data about oneself to grow in self-knowledge.<sup>38</sup>

On the other hand, knowledge is power. Governments have known this since long before the digital age. The Domesday Book and the secret police file catalogue information on people and their activities. The census, from the age of the punch card on, added database structure. These are the tools of rational administration, the essential inputs to bureaucracy and the extension of governmental power. On the one hand, this facilitates technocratic expert administration; on the other hand, punch-card technology helped organize the deportation and execution of Jews during the Holocaust.<sup>39</sup> Sorting people based on their

---

37. See *Privacy, Editing, Tagging, and Abuse*, FACEBOOK HELP CENTER, <http://www.facebook.com/help/?page=831> (last visited Mar. 11, 2011).

38. See GORDON BELL & JIM GEMMELL, *TOTAL RECALL: HOW THE E-MEMORY REVOLUTION WILL CHANGE EVERYTHING* 127 (2009).

39. See EDWIN BLACK, *IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE*

characteristics is a form of comprehensive control over them.<sup>40</sup>

The fear of control based on personal characteristics is also central to debates over personalized, targeted advertising.<sup>41</sup> What some authors see as empowerment, others see as manipulation. The advertising firm that builds a profile of your browsing habits (even, perhaps, if it can't identify you by name) nonetheless uses that personal profile to mark you and market to you. It uses that knowledge—which is made specific and actionable by the database entry—to exert power over you, possibly to your disadvantage.

Finally, some go a step further and argue that being represented in a database can be intrinsically objectifying. It flattens out one's identity to the standardized forms supported by the system. When protesters marched against computerization in the 1960s, with shouts that people were not to be "folded, spindled, or mutilated," this was the idea at work.<sup>42</sup> It is possible to argue that being represented in a database is intrinsically demeaning to one's human dignity. It strips out the respect for your personhood that demands you be recognized as a full, worthy, complex *person*, not just a reductive set of binary digits.

## CONCLUSION

This has been an essay about representing people in databases. I have argued that the transition from unstructured data to structured data is of critical importance for thinking about privacy and social interactions. There are echoes of at least three previous shifts in this transition: the introduction of print, the growth of bureaucracy, and the rise of digital media. All three of them have reworked the relationships of individuals to each other, and to the larger institutions that make up their worlds: communities, companies, and countries. The use of unique identifiers as the keys to structured databases about people will have its own dramatic consequences.

Another computer science term, this one from the field of programming languages, is suggestive of the values at stake. One sometimes says that a system which directly represents certain things treats them as "first-class objects."<sup>43</sup> One computing website explains

---

BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION 44 (2001).

40. See OSCAR H. GANDY JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* 134 (1993).

41. See, e.g., Tal Z. Zarsky, "Mine Your Own Business!": *Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 *YALE J.L. & TECH.* 1, 50-53 (2002).

42. See Steven Lubar, "Do Not Fold, Spindle or Mutilate": *A Cultural History of the Punch Card*, 15 *J. AMER. CULTURE* 43, 46-48 (2004).

43. See MICHAEL L. SCOTT, *PROGRAMMING LANGUAGE PRAGMATICS* 141 (2d ed. 2006); HAROLD ABELSON ET AL., *STRUCTURE AND INTERPRETATION OF COMPUTER*

that an element in a programming language is first-class “when there are no restrictions on how it can be created and used.”<sup>44</sup>

For example, in some programming languages, like C, functions are not first-class. Any subcomputation that the program will carry out must be specified in advance by the programmer, and there are significant limits on how functions can be stored, modified, and passed around. In other programming languages, like Scheme, functions are first-class: the computer treats them just like it would any other kind of data, like a number or a binary true/false. This leads to great flexibility. Scheme programmers can add new functionality on the fly as the program runs; they can do clever things with functions that C programmers can only mimic imperfectly and at much greater length.<sup>45</sup> It is easier to work with and reason about functions in Scheme than in C, because functions are first-class in Scheme and not in C.

People are first-class objects on Twitter: it has the capacity to distinguish and reason about them. The same is true in the many other systems that give people unique identifiers as a way of representing them in databases. Both halves of the phrase are illuminating. On the one hand, people are truly *first-class*: this representation enables useful features that connect directly to these individuals’ wants and needs. On the other, people are also *objects*: when these systems represent people, it is often without their knowledge or consent.

I have argued that treating people as first-class objects—representing them with digital identifiers—has significant technical and social consequences. Perhaps it should have legal consequences as well. We should expect the creators of these first-class objects to take care to treat people with the respect and concern the name suggests they deserve.

---

PROGRAMS 76 (2d ed. 1996); Christopher Strachey, *Fundamental Concepts in Programming Languages*, in 13 HIGHER-ORDER & SYMBOLIC COMPUTATION 11, 32–34 (2000).

44. *First Class*, CUNNINGHAM & CUNNINGHAM, INC., <http://www.c2.com/cgi/wiki?FirstClass> (last visited Mar. 11, 2011).

45. *See, e.g.*, DANIEL P. FRIEDMAN ET AL., ESSENTIALS OF PROGRAMMING LANGUAGES 24–25 (1992) (“First class procedures contribute greatly to the expressive power of a language.”).



# THE BROADCASTERS' TRANSITION DATE ROULETTE: STRATEGIC ASPECTS OF THE DTV TRANSITION

JAMES MILLER & JAMES E. PRIEGER\*

Furthermore, we expect that many stations will transition early and begin operating their final post-transition facilities in advance of the deadline and the onset of the winter months.<sup>1</sup>

|   |  |     |
|---|--|-----|
| INTRODUCTION.....   |  | 438 |
| I. THE BROADCAST TELEVISION MARKET .....  |  | 440 |
| A. <i>Regulatory Aspects</i> .....  |  | 441 |
| B. <i>Wireless Engineering and Physics</i> .....                                |  | 446 |
| C. <i>Industrial Organization</i> .....   |  | 448 |
| 1. The Evolution of the Networks and the Ownership<br>Cap.....                  |  | 449 |
| 2. Current Organization of the Industry .....                                   |  | 453 |
| II. THE SWITCH TO DTV .....   |  | 455 |
| A. <i>The Development of the DTV Standard</i> .....                             |  | 455 |
| B. <i>The Long, Slow March toward Transition</i> .....                          |  | 459 |
| 1. Changes in Power Requirements and Spectrum<br>Allocation.....                |  | 459 |
| a. <i>Existing License Holders</i> .....  |  | 459 |
| b. <i>Reallocations and New Users</i> .....                                     |  | 461 |
| 2. The Mandatory Transition to DTV and Cessation of<br>Analog Broadcasting..... |  | 462 |

---

\* James Miller is an Adjunct Professor of Law at American University, Washington College of Law and a Senior Attorney Advisor at the Federal Communications Commission. JamesMillerEsquire@gmail.com. James E. Prieger is an Associate Professor of Public Policy at Pepperdine University, School of Public Policy. James.Prieger@pepperdine.edu. We thank Michelle Connolly, Evan Kwerel, Jonathan Levy, Harold Furchtgott-Roth, Robert Weller, and participants at the 2009 Telecommunications Policy Research Conference for helpful comments, and David Mansdoerfer, Kevin Chlebig, and James Bieber for their research assistance. The opinions expressed (and any errors) are those of the authors and do not necessarily represent the views of the Federal Communications Commission, the United States Government, or any of the commenters.

1. Third Periodic Review of the Comm'n's Rules and Policies Affecting the Conversion To Digital Television, *Report & Order*, 23 FCC Rcd. 2994, 3017 ¶ 41 (2007) [hereinafter Third Review R&O].

|      |  |     |
|------|--|-----|
|      | <i>a. Legislative History of the DTV Transition</i> .....  | 463 |
|      | <i>b. FCC Rules for Transitioning</i> .....                | 465 |
| III. | STRATEGIC CONCERNS OF THE DTV TRANSITION .....             | 469 |
|      | <i>A. The Costs of the Transition for Stations</i> .....   | 470 |
|      | <i>B. Other Strategic Aspects of the Transition</i> .....  | 472 |
|      | <i>C. Economic Models of the Transition Decision</i> ..... | 473 |
|      | <i>D. Decision Theoretic Model</i> .....                   | 473 |
| IV.  | GAME THEORETIC MODEL .....                                 | 475 |
| V.   | EMPIRICAL EXAMINATION OF THE TRANSITION .....              | 477 |
|      | <i>A. Data</i> .....                                       | 477 |
|      | 1. Stations' Decisions and Characteristics .....           | 477 |
|      | 2. Market Information .....                                | 479 |
|      | <i>B. Empirical Results</i> .....                          | 480 |
|      | 1. Market Level Analysis .....                             | 480 |
|      | 2. Individual Stations' Decisions.....                     | 483 |
|      | <i>a. Preliminary Analysis</i> .....                       | 483 |
|      | <i>b. Regression Analysis</i> .....                        | 484 |
|      | CONCLUSIONS .....  | 490 |

## INTRODUCTION

The analog to digital “DTV transition” recently completed in the U.S. was a technological event unprecedented in scale in the broadcast television industry, touching nearly every American household directly or indirectly. Consumers’ demand for the new digital television (“DTV”) services, which have a sharper picture, smoother motion, better sound, and multiple sub-channels providing more viewing options, reflects the changing face of media delivery and consumption. On June 12, 2009, the last full-power television stations in the U.S. ceased over-the-air transmission of analog programming.<sup>2</sup> Today, all full-power stations transmit only DTV. The date was the culmination of more than ten years of complex regulatory decisions that provided broadcast station managers with varying regulatory conditions for voluntary transitioning and multiple mandatory cutoff dates.

---

2. In addition to the licensing of full-power stations, the FCC has licensed low-power television (“LPTV”) service since 1982, and more than 2,100 LPTV stations are now in operation. LPTV stations “provide opportunities for locally-oriented television service in small communities”; see *FCC Consumer Advisory: The DTV Transition and LPTV/Class A/Translator Stations*, FED. COMM’N COMM’N (Aug. 19, 2009), <http://www.fcc.gov/cgb/consumerfacts/DTVandLPTV.html>. The June 2009 DTV transition deadline did not apply to LPTV stations, although the FCC has stated that it will eventually require these stations to transition as well. We do not consider LPTV stations further in this article.

Stations around the nation transitioned individually and in varying degrees of coordination with each other, both in the local markets and throughout national networks. Facing engineering and economic concerns that could change their costs and revenue dramatically, stations acted in response to both market and regulatory forces. In this article, we identify and describe the various forces that influenced the DTV transition. We look at both the big picture of how the transition fits into the history of broadcasting in the U.S. and a detailed examination of the stations' final decisions regarding when to switch. In the latter, we focus on the economic and strategic aspects of the stations' business decisions, modeling their choices with tools from decision theory and game theory. In particular, our empirical examination looks at the stations' decisions whether to switch off analog broadcasting on February 17, 2009, the planned transition date until Congress delayed the deadline, or whether to continue to broadcast in analog until a later date. Despite the FCC's expectation at the end of 2007 that many stations would transition even before February 2009, quoted at the beginning of this article, most did not. We examine both theory and data to explore the decision making process of broadcast station managers facing a choice of when to switch to all-digital broadcasting.

The inherent tradeoff between switching earlier or later depends on the costs and benefits of switching to DTV. Broadcasting in DTV requires much less power than in analog, and the electricity savings can be substantial. Balancing the cost savings are fears that technical problems or changing broadcast footprints could cost a station viewership, and therefore advertising revenue. In the decision theoretic model we develop, a station's management considers only its own costs and the effect of its own decision on its viewership when deciding to switch early. However, fears of losing viewers are heightened if other stations in the local market do not also switch to DTV early, because rival stations might gain the lost analog viewers at least temporarily, and perhaps permanently due to habit-formation. Thus, each station must consider not only its own costs and revenues, but also the decisions made by the other stations. The game theoretic model builds on the simpler decision theoretic model to incorporate strategic thinking on the part of the station. In the game, a station manager considers the impact of other stations' decisions on its profit when making its choice.

The models predict that stations delay transition when they would see only small cost savings from transitioning relative to their expected lost revenue. In the game, such cases can become a classic Prisoners' Dilemma, wherein each station would like to lower its costs but neither

does in equilibrium.<sup>3</sup> When, on the other hand, stations face large cost savings from switching early relative to the expected loss of viewers when transitioning (in the decision model) or the expected gain of viewers from the other stations from delaying (in the game), stations switch early.

These outcomes from the models suggest several observable implications, which we explore and test using the stations' decisions and other data from the television broadcasting industry. In general, both casual and more formal econometric examinations of the data yield results that are in line with the predictions of the models. The results indicate that station managers indeed were thinking strategically when they made their transition decisions and were not merely considering their own cost savings apart from what other stations were doing. The results thus provide insight into the stations' decision-making process, which can help market observers and regulators better understand the calculus of the industry.

The article is organized as follows. Section II contains background information on the broadcast television market, covering its regulation, engineering aspects, and the organization of the industry. Section III discusses the development of the DTV standard and the long process of the DTV transition in the U.S. Section IV presents the financial and strategic considerations that factored into a television station's decision of when to turn off analog broadcasting. Section V introduces our economic models of the transition decision and derives testable implications. The models draw on both decision theory and game theory. Section VI introduces the data we collect on the U.S. broadcast television market and tests the predictions of the economic models with simple statistical analysis and with regression analysis. A final section concludes.

## I. THE BROADCAST TELEVISION MARKET

We begin by explaining the history, regulatory oversight, and current state of the broadcast television market in the U.S., to set the stage for the examination of the strategic aspects of the stations' decisions regarding switching to DTV.

---

3. The Prisoners' Dilemma refers to a class of games where each player's best individual strategy is to choose an action that is the opposite of the action that the players would agree to play if they could coordinate their actions. The Prisoners' Dilemma is thus an archetype of situations in which individual incentives lead to an inefficient equilibrium, compared to the (unsustainable) cooperative outcome. For a non-technical introduction to the Prisoners' Dilemma and its influence on public policy, see generally WILLIAM POUNDSTONE, PRISONER'S DILEMMA (1992).

### A. *Regulatory Aspects*

The recent transition of broadcast television from an analog to a digital technical standard is but the latest policy action in response to an important aspect of the industry present throughout its history: the high demand for the airwaves in the presence of competing interests. From its inception, both industry and government recognized the power of broadcast TV to reach mass markets, which created high demand for use of the radio spectrum.<sup>4</sup> Policymakers' desire to maximize the benefits from the use of the airwaves—a scarce resource—requires periodic rebalancing between the accommodation of incumbent technologies and the movement toward next-generation, state of the art technology. For almost a century, the evolution of the broadcast industry has been shaped by regulation.

The early age of broadcasting—at first, audio only—was a chaotic time, full of exciting advancements in technology and great experimentation. Initially, the only limitations on use of radio spectrum were those imposed by the state of the technology and laws of physics. Absent a regulatory structure, radio experimenters pushed the limits of the technology into areas that profoundly impacted commerce, entertainment, and the public good. Having played a role in both contributing to<sup>5</sup> and averting<sup>6</sup> major shipping disasters in the early 20th century, the use of wireless spectrum faced increased scrutiny from Congress. With the passage of the Radio Act of 1912, the federal government first established a system of “licensing” the use of radio spectrum under the Commerce Department, largely for reasons of maritime safety.<sup>7</sup> In addition to providing a means to check users'

4. Radio spectrum refers to the portion of the electromagnetic spectrum composed of frequencies between 3kHz and 300 GHz, those best suited for communications use. Airwaves used for what consumers think of as “radio broadcasting” (i.e., AM, FM, and now HD radio) compose only a small subset of radio spectrum.

5. Lack of coordination between the shipboard radio operators and the bridge was a contributing factor in the sinking of the RMS *Titanic*. See ROBERT D. BALLARD & RICK ARCHBOLD, *THE DISCOVERY OF THE TITANIC* 20 (1987).

6. After the actions of a radio operator saved the lives of 1,200 victims of a shipping accident in 1909, Congress passed the Wireless Ship Act. The 1910 law required radio equipment with a range of at least one hundred miles to be installed in all U.S. ships carrying over fifty passengers and traveling over two hundred miles off the coast. See HUGH RICHARD SLOTTEN, *RADIO AND TELEVISION REGULATION: BROADCAST TECHNOLOGY IN THE UNITED STATES 1920–1960* 6-8 (2000).

7. Observers of the events leading up to the loss of life in the sinking of the RMS *Titanic* urged changes in the U.S. and internationally to tighten procedures for the use of radios on vessels. Congress passed the Radio Act of 1912 largely in response to these concerns. The Act required all seafaring vessels to maintain constant radio watch and to keep in contact with nearby ships and coastal radio stations. The U.S. law mirrored the international treaty law negotiated in London at the International Radiotelegraphic Convention in 1912. See *Radio*

compliance with the legislation, the licenses served as a precursor to a broader notion of the federal government's ownership of the airwaves. Licensing constituted a system of government grants that constituted both permission to use spectrum under certain conditions, as well as rights to certain protections from "interference."<sup>8</sup>

By the early 1920s, the use of radio technology had expanded so rapidly that more than 500 broadcasters filled the country on a single frequency.<sup>9</sup> The growth of broadcasting occurred despite the fact that the Radio Act of 1912 did not anticipate broadcasting and that broadcast licensing was initially limited to two frequencies—one of which was reserved for crop reports and weather forecasts.<sup>10</sup> Significant court losses for the executive branch of the federal government, the growing economic value of and demand for spectrum, and the mounting concerns over interference and disruptions of the expectations of use of spectrum all challenged the early regulatory structure.<sup>11</sup> These and other factors drove the passage of the Radio Act of 1927 and its successor legislation, the Communications Act of 1934, which established the Federal Communications Commission ("FCC") as the regulator of broadcast and other uses of radio spectrum.<sup>12</sup>

The broad goals Congress defined for the FCC in the Communications Act of 1934 were matched by the far-reaching jurisdiction it granted to the agency. From its inception, the FCC regulated both market and engineering aspects of broadcast use of

Act, Pub. L. No. 62-264, 37 Stat. 302 (codified at 47 U.S.C. §§ 51-63 (1912), *replaced by* Communications Act of 1934 (codified as amended in scattered sections of 47 U.S.C.)).

8. Hazlett and other commentators observe that the rights and responsibilities associated with spectrum use were of chief concern at the time. *See* Thomas Hazlett, *The Rationality of U.S. Regulation of the Broadcast Spectrum*, 33 J.L. & ECON. 133, 145 (1990).

9. *See id.*

10. The 1912 Act delegated the regulatory powers over radio communication to the Secretary of Commerce and Labor. *See* 47 U.S.C. §§ 51-63 (1912).

11. The Secretary of the Department of Commerce, future president Herbert Hoover, played a strong role in shaping radio, despite Court losses that limited federal jurisdiction over radio licensing. In particular, the Court's invalidation of Hoover's denials of broadcast licenses for lack of standards, and later for federal jurisdiction outright under the existing statute hastened the legal changes establishing the modern federal regulatory structure for radio use. *See* *Hoover v. Intercity Radio Co.*, 286 Fed. 1003 (D.C. Cir. 1923); *United States v. Zenith Radio Corp.*, 12 F.2d 614 (N.D. Ill. 1926). The decision in *Zenith Radio* marked a period of "breakdown of the law[.]" described by some commentators as the death-knell of the burgeoning private market and judicial adjudications approaches, announcing a new federal "command and control" approach to spectrum management. *See* Hazlett, *supra* note 8, at 133-175 (discussing the history of market mechanisms for spectrum use and rejection in favor of the federal regulatory "command and control" approach).

12. Communications Act of 1934 (codified as amended in scattered sections of 47 U.S.C.).

spectrum.<sup>13</sup> Declaring that, “[n]o person shall use or operate any apparatus for the transmission of energy or communication or signal by radio . . . except under and in accordance with the Act and with a license . . . [.]” Congress firmly established federal ownership of the airwaves by fiat.<sup>14</sup> Congress intended unambiguously to bring radio use under federal control in order to encourage a greater and more effective use of radio “in the public interest, convenience, or necessity,” while at the same time prohibiting outright private ownership of spectrum.<sup>15</sup>

Under this Congressional mandate, and incorporating prior broadcasting determinations made under the 1927 Act by the Federal Radio Commission, the FCC implemented a variety of regulatory policies intended to foster the continuing growth of broadcasting and prevent interference between stations. After the FCC adopted its “chain broadcasting” rules in 1941, the modern regulatory framework of licensing broadcast stations geographically by service, frequency, and power, including limitations on which parties may hold licenses and procedures for denying or revoking licenses, was largely in place.<sup>16</sup> The rules established the market structure that remains today. In cases that challenged the FCC’s power to promulgate rules related to chain broadcasting by networks of stations, the Supreme Court upheld the

---

13. The FCC’s authority under 47 U.S.C. § 302(a) to “make reasonable regulations” that were “consistent with the public interest, convenience, and necessity” was not limited solely to the statutory provisions enumerated in the Communications Act. *See Nat’l Broad. Co. v. United States*, 319 U.S. 190, 217 (1943) (upholding the broad reading of the FCC’s regulatory power as extending beyond the technical engineering characteristics of radio spectrum management).

14. Communications Act of 1934, 47 U.S.C. § 301.

15. *Id.* § 307; *see also Id.* (providing for the use of radio frequencies under a license “but not the ownership thereof” so that “no such license shall be construed to create any right, beyond the terms, conditions, and periods of the license”).

16. Report on Chain Broadcasting: Commission Order No. 37, 6 Fed. Reg. 2282 (May 2, 1941), *modified*, Supplemental Report on Chain Broadcasting (Oct. 11, 1941), *appeal dismissed sub nom.* *Nat’l Broad. Co. v. United States*, 47 F. Supp. 940 (1942), *aff’d*, *Nat’l Broad. Co. v. United States*, 319 U.S. 190, 213-219 (1943) (discussing the background to the Commission’s broadcast licensing practices and policies at the time of the adoption of the chain broadcasting rules). Six rules related to network-station relationships and media ownership were originally adopted in the Report on Chain Broadcasting, and subsequently applied to the regulation of television broadcasting, but remained for many years a hotly debated topic. *See* Amendment of Part 3 of the Comm’n’s Rules, 11 Fed. Reg. 33 (Jan. 1, 1946) (applying the network radio rules to television networks); *see also The Impact of the FCC’s Chain Broadcasting Rules*, 60 YALE L. J. 78, 87-88 (1951) (describing the impact of the rules ten years after the adoption as “network revenues have soared, broadcasters have more than trebled in number, any diminution in sustaining programs can more accurately be attributed to increased expenditure for advertising, and government operation of radio is no closer today than ever” but arguing a revamping of the rules was crucial because of continuing concerns); HERBERT H. HOWARD, MULTIPLE OWNERSHIP IN TV BROADCASTING HISTORICAL DEVELOPMENT AND SELECTED CASE STUDIES 31, 34 (1979).

FCC's flexibility in implementing its broad mandate.<sup>17</sup> The Court concluded that the FCC's jurisdiction was not limited to the engineering aspects of radio use, but instead granted comprehensive power to promote and realize the vast potentialities of radio through "such rules and regulations[,] restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of th[e] Act."<sup>18</sup>

The advent of television created new challenges for regulation. Initially, the FCC classified the licensing of broadcast television as "experimental," mirroring the nascent state of the technical art at the time. TV broadcast's first home was in the very-high frequency ("VHF") portion of the spectrum.<sup>19</sup> The technical standards the FCC has selected have always reflected difficult balances between feasibility of existing state of the art, accommodation of incumbent technologies, and the need to maximize the beneficial use of the radio spectrum. The great diversity of technical solutions for a "television" system with the live transmission of sound and moving images that simulated motion (at least 12.5 frames per second) drove the FCC to address the technical conflicts among companies seeking to introduce nationwide service. The FCC formed the National Television System Committee ("NTSC") in 1940 to select a technical standard. In 1941, the FCC commenced licensing commercial broadcast television stations under the committee's adopted standard for black-and-white television, the NTSC Standard.<sup>20</sup>

Technical advancement in color technologies later required the FCC to explore a new standard. In 1948, the FCC formed its Joint

17. Report on Chain Broad., *supra* note 16; *see also Nat'l Broad. Co.*, 319 U.S. at 213-19.

18. *Nat'l Broad. Co.*, 319 U.S. at 217 (citing the statute).

19. *See infra* Part I.B.

20. On May 3, 1941, the Commission released its April 30, 1941 Order that adopted the monochrome NTSC standard. Rules Governing Standards and High Frequency Broadcast Stations, 6 Fed. Reg. 2282 (May 6, 1941); *see also* Amendment of Section 3.606 of the Comm'n's Rules and Regulations, 41 F.C.C. 148 (1952). Amendment of the Comm'n's Rules, Regulations, & Engineering Standards Concerning the Television Broad Service, Docket No. 9175. Utilization of Frequencies in the Band 470 to 890 Mcs for Television Broad, 41 F.C.C. 1, 3 ¶ 8 (1950); Final Report of Nat'l Television System Comm., NTSC-G-421, at 5 (July 21, 1953) [hereinafter Report of NTSC on Color Standard] (discussing that the rules establishing the NTSC monochrome standard became effective July 1, 1941 and other history of NTSC's work with the FCC in developing the first monochrome NTSC television standard). Discussions between the then FCC Chairman Fly and the Radio Manufacturers Association Director, Dr. W.R.G. Baker (also Vice President of General Electric Corporation) indicated that a collaborative group focused on "the scientific development of the highest standards within reach of the industry's experts" could resolve the divided opinions on the engineering of television and facilitate the Commission's goal of a standard that could bring about a full commercialization of the technology. *See* Order 65 Setting Television Rules and Regulations for Further Hearing, Dkt. No. 5806 (May 28, 1940); *see also* Report of NTSC on Color Standard, at 3-4.

Technical Advisory Committee (“JTAC”).<sup>21</sup> The FCC provisionally approved a JTAC recommendation for a color standard that would have taken advantage of new technologies exploiting the ultra-high frequency (“UHF”) band. However, the JTAC recommendation was not backward compatible with the existing NTSC black-and-white standard. If pursued, the FCC would have allowed the prior standard to become obsolete as consumers purchased color televisions that would use different spectrum and an incompatible technical standard—naturally making it possible to reclaim the VHF band as attrition occurred.

In the two years the color standard was being considered, the number of black and white NTSC-compatible televisions in the marketplace exploded from under a million sets in 1948 to over 10 million by 1951.<sup>22</sup> Recognizing that making the millions of existing sets in the market obsolete would constitute a significant burden for consumers, the FCC reconvened the NTSC in 1950, recommending that the Committee identify a “compatible color” standard.<sup>23</sup> Compatibility would protect the value of the investment consumers had made in the still relatively new NTSC black and white TV technology. In December 1953, the NTSC adopted a compatible standard.<sup>24</sup> Thus, respecting consumers’ existing investments in equipment was a deciding factor even in the selection of the modern analog television NTSC standard.<sup>25</sup> The FCC would again wrestle with this issue in the transition to DTV.

21. ENGINEERING ASPECTS OF TELEVISION ALLOCATIONS, REPORT OF THE TELEVISION ALLOCATIONS STUDY ORGANIZATION TO THE FEDERAL COMMUNICATIONS COMMISSION 39 (Mar. 16, 1959) (discussing the history of JTAC and work developing studies on television engineering).

22. J.Y. Smith, *Milton Berle, ‘Mr. Television,’ Dies at 93: Comic Sparked American Love Affair with Small Screen*, WASH. POST, March 28, 2002, at A1.

23. On June 18, 1951 the NTSC reorganized with nine Panels numbered 11-19 and “devoted its efforts solely to the significant and highly challenging technical problem of achieving the best possible color television signal specification; specifications capable of creating a practical color transmission utilizing as a foundation, the existing monochrome standards.” Report of NTSC on Color Standard, *supra* note 20, at 13.

24. Amendment of the Comm’n’s Rules Governing Color Television Transmissions, 41 F.C.C. 658 (1953) (discussing the improvements to the NTSC standard supporting color television broadcasting). See also Nat’l Television Sys. Comm. for Adoption of Transmission Standards for Color Television, NTSC-G-378 (July 21, 1953). The NTSC reviewed independently and separately the work of the respective panels in 25 meetings and voted on July 21, 1953 authorizing and directing the Chairman to file the petition with the FCC proposing the adoption of its NTSC signal specification as the standard for commercial color television broadcasting. Report of NTSC on Color Standard, *supra* note 20, at 15.

25. The first broadcast of a program using the NTSC “compatible color” system was an episode of NBC’s *Kukla, Fran and Ollie* on August 30, 1953. *60<sup>th</sup> Anniversary of Kukla, Fran, and Ollie with Burr Tillstrom*, SENIOR CONNECTION, <http://www.seniorconnectionnewspaper.com/articles/2009/kukla.asp> (last visited Apr. 20, 2011). While the broadcast was announced to the public it could only be seen in color at the network’s facility.

## B. *Wireless Engineering and Physics*

To understand the financial and strategic incentives facing television stations to switch to DTV, one must understand some of the engineering and physical principles involved with broadcasting. Two separate tracks of technology, 1) the generation and display of TV images using television cameras and video monitors (i.e., “TV sets”), and 2) the radio-frequency (“RF”) transmitters and receivers that carry signals through the air, had evolved by the early 1930s to enable the birth of the new broadcasting industry. The early technology made use of techniques and fundamental physics that still apply today. These engineering fundamentals continue to play a role in the decision making of broadcast entities.

Major discoveries and advances of the early 20th century in the areas of physics and material science provided the technical foundations for television broadcasting for the next 75 years. Techniques for capturing and reproducing graphical images made use of both mechanical and electronic components, but by the time of the Communication Act of 1934, the fundamental technologies necessary for modern television using a solely electrical process had already emerged.<sup>26</sup> The radio engineering techniques to deliver the prepared moving images and sound also advanced greatly in the early age of radio. The ability to manipulate radio waves to carry information had developed by the time the regulatory structure congealed in the early 1930s. World War II spurred great advances in wireless engineering in the 1940s, making the technology ready for prime time.<sup>27</sup>

A complete discussion of television broadcast engineering is unnecessary for present purposes, but a basic explication of three fundamental RF engineering considerations illustrates how certain technical aspects of the DTV transition are relevant to the strategic interests of broadcast entities. Each consideration stems from the physical aspects of how radio waves propagate and are manipulated to carry information.

First, a transmission effectively loses power as it travels from its source. The loss implies that the power level transmitted from the transmitter (the antenna) defines the geographic area in which reception is possible.<sup>28</sup> The more power transmitted, the greater the area in which

---

26. See GARY R. EDGERTON, *THE COLUMBIA HISTORY OF AMERICAN TELEVISION* 50 (2007).

27. Pun intended.

28. The reduction of power density as radio waves propagate from their source, known as *path loss*, results from a variety of conditions, including spreading losses, absorption losses, and diffraction losses. Radio applications typically evaluate “path losses” in decibels (“dB”). A

reception of the signal is possible. Broadcast TV transmitters typically transmit thousands or millions of watts and provide coverage over hundreds of square miles.

Second, spectrum propagates through space undulating in waves. The physical properties of spectrum differ with the length of the waves. In particular, waves of longer length (i.e., of greater “wavelength”) travel farther than those of shorter length given that both are transmitted at the same power. Radio waves can also be characterized in terms of number of undulations the wave completes in a given period (i.e., the “frequency”), typically measured in Hertz (“Hz”).<sup>29</sup> Television stations broadcast signals to viewers over a wide swath of frequencies.<sup>30</sup> As mentioned above, TV broadcasting first made use of the VHF band. Signals in this band have long wavelengths that travel the farthest at the lowest power levels and are most able to reach viewers in mountainous regions or areas with dense foliage. Television broadcast signals in the higher-frequency UHF band typically require more power to provide service over the same area as an equivalent VHF signal.<sup>31</sup> However, because of the number of common sources of significant interference in the VHF band, UHF broadcast signals benefit from a more interference-free environment. The range of broadcast frequencies is divided into “channels” corresponding to the 6 MHz increments to which licenses are allocated. VHF stations broadcast over channels 2 through 13, and UHF stations transmit in channels 14 and above.<sup>32</sup>

Third, techniques for manipulating (i.e., “modulating”) radio waves to carry information exploit different properties of radio waves. For example, amplitude modulation (“AM”) and frequency modulation (“FM”), important standards in radio broadcasting, encode information by manipulating the power level and wavelength of radio waves

common expression for free space path loss (“FSPL”) using reads:

$$\text{FSPL} = 20\log_{10}(d) + 20\log_{10}(f) + 32.44$$

where  $f$  is frequency in MHz,  $d$  is distance in km, and loss is measured in dB. See CLINT SMITH & DANIEL COLLINS, 3G WIRELESS NETWORKS 388 (2002).

29. The relationship between frequency and wavelength is:  $f = c/\lambda$ , where  $f$  is frequency in Hertz (Hz, in cycles per second),  $\lambda$  is the wavelength in meters, and  $c$  is the speed of light (approximately equal to  $3 \times 10^8$  meters per second).

30. The lowest frequency currently allocated for broadcast in use (for channel 2 in the VHF band) is 54 MHz and the highest frequency (for channel 51 in the UHF band) is 698 MHz.

31. The requirement for higher power for UHF frequencies is discussed in Appendix A of the OET Bulletin No. 69 and the Advanced Television System’s Sixth Further Notice, as the “dipole factor.” See generally *Longley-Rice Methodology for Evaluating TV Coverage and Interference*, FED. COMM’NS COMM’N (Feb. 6, 2004).

32. The FCC first adopted these channel allotments in an order in 1952. See Amendment of Section 3.606 of the Comm’n’s Rules and Regulations, *Sixth Report & Order*, 41 F.C.C. 148 (1952). Several changes in allotments were subsequently made.

respectively. An NTSC broadcast comprises an AM video signal (at 30 frames per second) and an FM audio signal. Information can also be encoded using different mathematical approaches to improve the performance, resiliency to interference, or other features. For example, DTV standards encode TV video and audio signals digitally using compression and error-correcting techniques similar to those used in modern consumer electronics equipment such as DVD players. Thus, DTV standards are referred to as “digital,” as opposed to the “analog” NTSC standard. Use of digital techniques makes it possible to carry more information than an NTSC system, and with higher reliability and at much lower power.

Regardless of the modulation or engineering technique used in the broadcast, the quality of TV reception is heavily dependent on the nature and quality of the TV receiver and antenna. The effectiveness of an antenna to receive TV signals depends, among other things, on whether the physical size of the antenna appropriately matches a multiple of the wavelength of the desired signal. In particular, an antenna designed to receive VHF signals does not work well at pulling in UHF stations, and vice versa. In some cases, consumers having antennas with only a VHF or UHF component would lack the ability to receive some DTV transmissions, which may make use of both bands. Moreover, the quality of a receiver can be even more important when overcoming certain kinds of interference or for quality demodulation of digital signals. Unlike reception of analog transmissions, which gradually fade to “snow” as quality degrades, DTV exhibits the “digital cliff effect,”<sup>33</sup> so-called because reception is either perfect or non-existent, with an abrupt transition between the two states. The greater importance of the quality of the receiving equipment, along with the digital cliff, means that the transition to DTV is attended with the potential loss of viewers of a broadcast station. As we discuss below, these considerations played a role in the calculus of stations deciding when to switch to DTV.

### C. *Industrial Organization*

The market structure, conduct, and performance of the broadcast television industry (collectively, its “industrial organization”) reflect both regulatory and business considerations. Predominant among these

---

33. See generally John Eggerton, *Klobuchar Warns of DTV ‘Cliff Effect’: Sen. Amy Klobuchar Writes FCC, NTIA to Reiterate Concerns About DTV ‘cliff effect’*, BROAD. & CABLE, Sept. 21, 2008; Glenn Doel, Workshop on Frequency Planning and Digital Transmission: DVB-T Transmission Systems (Nov. 23, 2004) (unpublished presentation), available at [http://www.itu.int/dms\\_pub/itu-r/oth/0C/07/R0C070000590006PDFE.pdf](http://www.itu.int/dms_pub/itu-r/oth/0C/07/R0C070000590006PDFE.pdf) (describing a “brick wall” effect).

considerations is the ownership structure of the entity holding the FCC license, the “station.” Media ownership restrictions are a complicated area of regulatory practice, but several considerations have influenced the TV broadcast market and the decision making of broadcast entities. In this section, we review the formation of the television networks and sketch a picture of competition in the industry today. Understanding the relationships among stations and the revenue sources for broadcasters is important for analyzing the incentives station owners faced regarding to transition to DTV.

### 1. The Evolution of the Networks and the Ownership Cap

After broadcast technologies became technologically viable, their popularity exploded and large capital backers began “[selling] gas stations and [buying] radio stations.”<sup>34</sup> Consolidation of the ownership of stations began with the very first commercial radio licensee, Westinghouse Electric, when in 1921 it added two additional stations to its original facility, KDKA Pittsburgh.<sup>35</sup> Consolidation of licenses increased the potential for advertising revenue and furthered stations’ financial growth. The development of networks of stations made “chain broadcasting” possible, in which media content could be broadcast simultaneously by multiple stations. Networks in this modern sense began in 1926 with the formation of the National Broadcasting Company (“NBC”) network, closely followed by Columbia Broadcasting System (“CBS”) in 1927.<sup>36</sup>

The formation of these networks depended on the use of telecommunications technology to connect the “chains” of stations, and the commercial relations between network owners and the stations controlled access to these fundamental tools. NBC’s owner, Radio Corporation of America (RCA, a subsidiary of General Electric), was initially unable to negotiate use of the high-quality voice telephone circuits necessary to connect its stations. AT&T, the owner of the telephony network supporting the circuits, refused to deal with RCA because AT&T owned a competing radio station network (WEAF).<sup>37</sup>

---

34. HOWARD, *supra* note 16, at 34. Use of radio in World War I advanced the art of radio considerably and accelerated its adoption; *see also* Nat’l Broad. Co., 319 U.S. at 211.

35. HOWARD, *supra* note 16, at 20; *see also* STEPHEN DAVIS, LAW OF RADIO 140 (1927).

36. HOWARD, *supra* note 16, at 20, 29.

37. The exhaustive NBC File of the Library of Congress contains press releases, fillings, personnel records and other items of interest from this period. *See generally* KATHLEEN B. MILLER ET AL., NBC: A FINDING AID TO THE NATIONAL BROADCASTING COMPANY HISTORY FILES AT THE LIBRARY OF CONGRESS, MOTION PICTURE, BROADCASTING AND RECORDED SOUND DIVISION (1999); *see also* Thomas H. White, *United States Early Radio History: Section 19, EARLY RADIO HISTORY*, <http://earlyradiohistory.us/sec019.htm> (last visited Feb. 22, 2010).

Economists refer to such denial of essential inputs by a vertically integrated firm (AT&T) to a downstream rival (RCA/NBC) as “foreclosure.” RCA found a solution to its quandary by buying the WEAF network from AT&T, thus destroying the latter’s incentive to foreclose. With the new acquisition, RCA formed NBC with the WEAF chain stations (shortly thereafter renamed the NBC-Red network) and its existing WJZ network (renamed the NBC-Blue network).

Not unlike its competitors, NBC’s interests and network focus were tied closely to the business strategies of its parent organization Radio Corporation of America (“RCA”), and its market dominance continued to draw the ire of competitors. In 1938, in response to a request by the Mutual Broadcasting System, the FCC commenced its first inquiry into competition in the broadcast industry, investigating the domination of the market by NBC and CBS.

In its 1941 report on Chain Broadcasting, the FCC expressed concern that

[C]ommon ownership of network and station places the network in a position where its interest as the owner of certain station may conflict with its interest as a network organization serving affiliated stations. The danger is present that the network organization will give preference to its own stations at the expense of its affiliates.<sup>38</sup>

The Commission also found that an organization operating multiple networks, such as RCA with its “two color” NBC networks, could result in an unfair competitive advantage over other networks.

In the report and through subsequent action in the 1940s, the FCC expressed its defining view that it had an obligation to restrict the number of commonly-owned stations, and to serve the public interest by preserving diversification in the ownership of networks and stations.<sup>39</sup> As stated in a later report,

The purpose of the multiple ownership rules is to promote diversification of ownership in order to maximize diversification of program and service viewpoint as well as to prevent any undue concentration of economic power contrary to the public interest.<sup>40</sup>

---

38. HOWARD, *supra* note 16, at 35 (quoting FCC, Report on Chain Broadcasting, Report, Dkt. No. 5060 (1941) (Washington U.S. Govt. Printing office)).

39. See FCC, Supplemental Report on Chain Broad. 14 (1941); 8 Fed. Reg. 16,005 (1943); Amendment of Part 3 of the Comm’n’s Rules, 11 Fed. Reg. 33 (Jan. 1, 1946).

40. Amendment of Sections 3.35, 3.240, and 3.636 of Rules and Regulations to Multiple Ownership of AM, FM, and Television Broadcast Stations, Report & Order, 18 F.C.C. 288,

Having noted that vertical integration of the network content distributor with the broadcast stations was firmly established, the FCC criticized the networks' practice of owning and operating numerous high-power stations. Such stations are known as "O&O" stations. The criticism of O&Os by the FCC led RCA to divest station ownership and network operations of its NBC Blue network of stations, albeit not until unsuccessfully challenging the FCC's authority to enforce its new policies. The Blue network, thereafter under new ownership, became the third independent national network under the moniker American Broadcasting Company ("ABC").<sup>41</sup>

The changes in the regulatory environment resulted in a cap on the number of stations a given entity could hold, and networks facing this limitation were forced to choose which O&Os to keep. At first, the cap was set at three stations,<sup>42</sup> but was soon raised to five.<sup>43</sup> Naturally enough, the networks focused on establishing ownership interests in the major TV markets, where they continue to hold their O&O stations today. In addition, mergers between networks or the holding of more than one network by an entity, known as the "dual network" rule, was also prohibited.<sup>44</sup> Nevertheless, networks continued to expand their content offerings throughout the nation through "affiliate" relationships with

291 (1953). *See also* Stuart Minor Benjamin, *Evaluating the Federal Communications Commission's National Television Ownership Cap: What's Bad for Broadcasting is Good for the Country*, 46 WM. & MARY L. REV. 439 (2004) (expressing a contrary view on the need for an ownership cap).

41. *Nat'l Broad. Co.*, 319 U.S. at 224 (concluding "that the Communications Act of 1934 authorized the Commission to promulgate regulations designed to correct the abuses disclosed by its investigation of chain broadcasting."). After internal NBC discussions dating back to 1932 and the separation of the NBC Blue and Red sales teams in 1939, NBC Blue operations had already been made independent in a newly created "Blue Network Company" by the time Supreme Court rendered its decision, and RCA subsequently filed its request to transfer and assign the network that the FCC approved on October 12, 1943.

42. Rules and Regulations Governing Experimental Television Broadcast Stations, 6 Fed. Reg. 2282, 2284-85 (1941) (codified at former 47 C.F.R. § 4.226)

43. Multiple Ownership, 9 Fed. Reg. 5442 (May 23, 1944). For a review of the changes in the national ownership cap over the years up to the passage of the Telecommunications Act of 1996, *see* 1998 Biennial Regulatory Review – Review of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, 15 FCC Rcd. 11,058, 11,066 § IV.a.1 (2000).

44. The dual network rule remained in effect until changes in the 1996 Telecommunications Act and FCC action 2001 restricted the scope of the rule. *See* 47 C.F.R. § 73.658(g) (2010) (prohibiting a television broadcast station from affiliating with a person or entity that maintains two or more networks of television broadcast stations unless such dual or multiple networks are composed of two or more persons or entities that, on February 8, 1996, were "networks" as defined in § 73.3613(a)(1) of the Commission's regulations (that is, ABC, CBS, Fox, and NBC); *see also* Amendment of Part 3 of the Comm'n's Rules, 11 Fed. Reg. 33 (Jan. 1, 1946) (establishing the "dual network" rule); Amendment of Section 73.658(g) of The Comm'n's Rules – The Dual Network Rule, *Report & Order*, 16 FCC Rcd. 11, 114 (2001).

independent stations. These affiliated stations contract with a network under a franchising agreement to broadcast the network's programming content while maintaining an independent ownership and management structure.

As demand for station licenses continued to swell after World War II, leading to the opening up of spectrum in the UHF band for broadcasting use, the FCC relaxed the ownership restriction to seven stations in 1954.<sup>45</sup> However, the FCC provided that no more than five VHF stations would be allowed. While the FCC differentiated the ownership restrictions for VHF and UHF channels in order to promote development of the spectrum newly available for broadcasting, entry of new UHF stations progressed slowly. UHF stations were often viewed as inferior to VHF even after technology shortcomings were addressed.<sup>46</sup> As discussed above, a UHF broadcast requires more power than a VHF broadcast, in addition to other engineering differences. The value of UHF station ownership was also lower because, until 1964 (when UHF tuner technology became required in all TV receivers), consumers had to buy a new antenna and either purchase a "TV-top converter" or a compatible TV receiver. As another case of a new broadcast technology requiring consumers to upgrade their home electronics equipment, UHF broadcasting was an exemplar of the 2009 U.S. DTV transition.<sup>47</sup>

The next change in the national television broadcast ownership rules was in 1984, when the common ownership of 12 stations was permitted.<sup>48</sup> The next year, the higher cap was limited by an "audience reach cap," by which the percentage of households able to view a network's O&O could be no more than 25 percent of the national viewing audience.<sup>49</sup> The numerical limit on the number of stations was eliminated in 1996 and the audience reach cap was raised to 35 percent.<sup>50</sup>

45. Amendment of Section 3.636 of the Comm'n's Rules and Regulations Relating to Multiple Ownership of Television Broad. Stations, *Report & Order*, 43 F.C.C. 2797 (1954).

46. UHF station management, technology, and culture has been lampooned in popular culture. See *UHF*, IMDB (1989), <http://www.imdb.com/title/tt0098546/> (last visited Mar. 1, 2010).

47. See All-Channel Receiver Act ("ACRA"), 47 U.S.C. § 303(s) (1964).

48. See Amendment of Section 73.3555 of the Comm'n's Rules Relating to Multiple Ownership of AM, FM and Television Broad. Stations, *Report & Order*, 100 F.C.C.2d 17 (1984).

49. See Amendment of Section 73.3555 of the Commission's Rules Relating to Multiple Ownership of AM, FM and Television Broadcast Stations, *Memorandum Opinion & Order*, 100 F.C.C.2d 74 (1985). Due to their technical disadvantages, UHF stations are attributed with only half of the audience they can reach for purposes of computing the cap. 2006 Quadrennial Regulatory Review—Review of the Comm'n's Broad. Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, *Report & Order & Order on Reconsideration*, 23 FCC Rcd. 2010, 2084 ¶ 142 (2007).

50. See Implementation of Sections 202(c)(1) and 202(e) of the Telecommunications Act

In 2003, the cap briefly rose to 45 percent,<sup>51</sup> but was reduced by Congress to 39 percent shortly thereafter.<sup>52</sup>

The import of network formation in the broadcast industry for the transition decisions concerns the locus of the decision-making. Managers of television stations that are O&Os of a network generally were not free to make their own decisions regarding when to transition to DTV, since such decisions were made at the corporate level of the network. Affiliated stations not owned by the network and other independent stations, on the other hand, had more leeway in choosing their transition timing. The distinction between the types of stations implies that it is important to control for whether a station is an O&O in the statistical regression we perform in section V.

## 2. Current Organization of the Industry

To understand what is at stake for the stations as they switch to DTV broadcasting, the most salient facts are that station revenue comes primarily from advertising, and that advertising revenue is driven by viewership. Advertising in broadcast television markets has traditionally been priced by CPP, the cost per point of Nielsen Media Research Company rating "points,"<sup>53</sup> although more recently the industry is shifting to more direct measures of "audience impressions" (i.e., how many times the commercial is likely to be viewed).<sup>54</sup> The broadcast television industry has bled viewer share to cable over the years. Although the Big Three networks (ABC, CBS, and NBC) saw their share of viewers fall from 70 percent in 1986 to 27 percent in 2006, with cable television picking up most of the lost audience, advertising revenue

---

of 1996 (National Broadcast Television Ownership and Dual Network Operations), *Order*, 11 FCC Rcd. 12,374 (1996).

51. See 2002 Biennial Regulatory Review—Review of the Commission's Broadcast Ownership Rules and Other Rules Adopted Pursuant to Section 202 of the Telecommunications Act of 1996, *Report & Order & Notice of Proposed Rulemaking*, 18 FCC Rcd. 13,620 (2003).

52. See Consolidated Appropriations Act, Pub. L. No. 108-199, tit. VI, § 629, 118 Stat. 3, 99-100 (2004).

53. Nielsen ratings are the industry standard to measure the viewership of a television program or station. A Nielsen "ratings point" represents one percent of the total number of television households in the relevant geography (the nation or a local market, depending on the context). Nielsen collects information on the viewing behavior of households and individuals through paper viewing diaries and electronic metering equipment in selected homes. Regardless of method, each household in the Nielsen panel provides about a week's worth of viewing information during the "sweeps" months of November, February, May and July. In some diary markets, additional months are surveyed as well. See *Television: How the Numbers Come to Life: Panels*, NIELSEN, [http://en-us.nielsen.com/tab/measurement/tv\\_research](http://en-us.nielsen.com/tab/measurement/tv_research) (last visited Mar. 1, 2010).

54. SNL KAGAN, *ECONOMICS OF TV PROGRAMMING & SYNDICATION* 55 (2007).

for the Big Three did not begin to fall until after 2006.<sup>55</sup> Part of the reason for the maintained levels of advertising revenue is that the networks have responded to lost viewing share by increasing the minutes of advertising each viewing hour.<sup>56</sup>

A network sells advertising to be aired on all of its affiliated stations, whether it owns the station or not. In 2009, advertising revenue for the five largest networks totaled \$21.9 billion.<sup>57</sup> Nearly all of this amount is generated by sales of broadcast advertising, although some of the network revenue also comes from ads sold for programs that are streamed online. The figure for 2009 was about 8 percent lower than it was the previous year.<sup>58</sup> The market share of advertising revenue was 27 percent for ABC, 29 percent for CBS, 20 percent for FOX, and 20 percent for NBC,<sup>59</sup> implying that there are four roughly equally sized competitors at the national level.<sup>60</sup> In the local markets, the viewing (and therefore the advertising revenue) shares may vary, but no network can own two stations in the same market unless one of the stations is not in the top four in terms of audience share, and there are more than seven other independent stations also in the market.<sup>61</sup>

In order to spread their revenue sources wider, networks also own shares in some of their programming series. Taking a stake in a series enables the network to profit from “aftermarket” revenue as well as from initial advertising sales. The additional revenue sources include broadcast syndication fees (domestic and international), “repurposing” fees from cable and direct broadcast satellite channels,<sup>62</sup> DVD sales, and video on demand.<sup>63</sup> The aftermarket revenue from a hit series is estimated to

55. *Id.* at 5; Brian Steinberg, *Most TV—Broadcast or Cable—Saw Ad Revenue Fall Last Year*, ADVERTISING AGE (Feb. 22, 2010), [http://adage.com/mediaworks/article?article\\_id=142244](http://adage.com/mediaworks/article?article_id=142244) (citing figure from Kantar Media). Some of the market share lost by broadcast TV migrated to direct broadcast satellite and programming services from broadband providers, such as Verizon’s FIOS and AT&T’s U-verse. See Tamara Chuang, *Cable TV Losing 1 Million Customers a Year*, ORANGE COUNTY REGISTER (May 22, 2009, 9:29AM), <http://gadgetress.freedomblogging.com/2009/05/22/cable-tv-losing-1-million-customers-a-year/13701/>.

56. SNL KAGAN, *supra* note 54, at 5.

57. Steinberg, *supra* note 55 (The figure includes all ad revenue, not just the season “upfront” commitments often cited in the industry press).

58. *Id.*

59. *Id.*

60. *Id.* The final 3 percent of advertising revenue earned by major networks in 2009 went to CW.

61. 2006 Quadrennial Regulatory Review, 23 FCC Rcd. 2010 (2007), *supra* note 49, ¶ 87.

62. Syndication means licensing “reruns” of a series to broadcast stations. Repurposing refers to moving content from the broadcast format to another modality such as cable.

63. SNL KAGAN, *supra* note 54, at 59. The networks first entered the video on demand market on a large scale around 2006 by selling programs on iTunes.

account for as much as 90 percent of the total (undiscounted) revenue stream, although aftermarket revenue composes much less of the whole revenue for non-hit series.<sup>64</sup>

More important for the empirical work below is the advertising revenue accruing to individual broadcast stations. Stations, even those affiliated with a network, offer their own commercial airtime—"spot advertising"—for purchase. Buyers of television spots are often local advertisers, but even when not, the network with which a station is affiliated is not allowed to control the rates for spot advertising.<sup>65</sup> Revenue earned directly by the stations from advertising is roughly equal to the amount earned by the networks' own ad sales. In 2009, sales of local and national spot advertising garnered stations an estimated \$24.1 billion.<sup>66</sup> As with the networks, advertising revenue for stations was down in 2009, falling 17 percent from the previous year.<sup>67</sup> While local stations also earn some revenue from retransmission agreements with cable television companies and online advertising, broadcast advertising still makes up about 97 percent of the average station's revenue.<sup>68</sup> Protecting this dwindling revenue stream was one of the prime concerns of station managers considering when to switch to DTV. The same is true of the network O&O stations, which are a profit center for the networks. While the major networks have only small profit margins, O&O stations have profit margins of 40 to 50 percent as recently as 2007.<sup>69</sup>

## II. THE SWITCH TO DTV

### A. *The Development of the DTV Standard*

Since the development of the engineering and regulatory structure

64. SNL KAGAN, *supra* note 54, at 16.

65. See generally B.D. McCullough & Tracy Waldon, *The Substitutability of Network and National Spot Television Advertising*, 37 QJ. BUS. & ECON. 3 (1998) (for discussion of how and why the FCC sought to ensure the survival of an independent advertising market outside the control of the networks).

66. Steinberg, *supra* note 55. Local spot advertising (about 55 percent of total spot advertising) appears only in a station's own market. National spot advertising appears in large portions of the country. A company might choose to advertise with a national spot instead of a national network commercial because it wants to target only hot, sunny states for a sunscreen ad, for example.

67. Michael Malone, *Study: Station Revenue Up 5.2% in 2010*, BROAD. & CABLE (Aug. 18, 2009), [http://www.broadcastingcable.com/article/327843-Study\\_Station\\_Revenue\\_Up\\_5\\_2\\_in\\_2010.php?rssid=20068](http://www.broadcastingcable.com/article/327843-Study_Station_Revenue_Up_5_2_in_2010.php?rssid=20068) (citing a study by SNL Kagan).

68. Katy Bachman, *Report: TV Stations Finding Multiple Revenue Streams*, MEDIAWEEK (Feb. 8, 2010), [http://www.mediaweek.com/mw/content\\_display/news/local-broadcast/e3ief7f94880dc0982e7611a33c5d5ad05c](http://www.mediaweek.com/mw/content_display/news/local-broadcast/e3ief7f94880dc0982e7611a33c5d5ad05c) (citing a study by SNL Kagan).

69. SNL KAGAN, *supra* note 54, at 61.

for broadcast television, the industry thrived in the U.S. for three quarters of a century. Six of those decades were under the NTSC color standard. Despite advances in technology that created opportunities to bring dramatic quality improvements to broadcast television, the NTSC analog standard remained largely unchanged into the 1980s. By then, however, the forces of change were already unleashed. The convergence of two factors, the increased demand for spectrum and the technological opportunities for advanced television content and devices, led to a 20-year process that culminated in the cessation of analog broadcasting on June 12, 2009.<sup>70</sup> The switch to DTV realized dramatic improvements in the efficiency of the use of radio spectrum, gave greater flexibility to broadcasters, and raised the quality of the television experience for viewers. This section recounts the history of the transition.

In the mid-1980s, Japanese electronics firms demonstrated high-definition TV (“HDTV”) technologies.<sup>71</sup> U.S. consumer electronics firms, already weakened from strong competition since the 1960s with Japanese firms, viewed HDTV as a new challenge.<sup>72</sup> In the 1980s, *Nippon Hoso Kyokai* (“NHK”), Japan’s national broadcasting company, began broadcasting their HiVision HDTV system, known in the U.S. as MUSE (Multiple sub-Nyquist sampling encoding). The popular and academic press used MUSE as an example of the resurgence of Japanese R&D and electronics that appeared to portend the passing of technological leadership from U.S. firms to overseas competitors.<sup>73</sup> Besides reasons of industrial policy, some commentators (as well as the U.S. Defense Department) also advocated for a homegrown HDTV standard for purposes of national security.<sup>74</sup> Furthermore, the significant

70. The Short-term Analog Flash and Emergency Readiness Act, Pub. L. 110-459, 122 Stat. 5121 (2008), was enacted prior to the enactment of the DTV Delay Act of 2009, Pub. L. No. 111-4, 123 Stat. 112 (codified in scattered sections of 47 U.S.C.), which changed the nationwide transition deadline from February 17 to June 12, 2009.

71. Although the public often conflates HDTV and DTV, the two need not be synonymous. HDTV refers to a higher definition picture quality than that provided by an NTSC(-like) standard. Many of the early HDTV proposals, including MUSE, involved analog systems. The ATSC standard adopted for DTV in the U.S. also includes HDTV.

72. See generally *The History and Politics of DTV*, CINEMASOURCE TECHNICAL BULLETIN 4 (2002); Jeffrey A. Hart, *The Politics of HDTV in the United States*, 22 POLY STUD. J. 213 (1994); WALTER B. EMERY, NATIONAL AND INTERNATIONAL SYSTEMS OF BROADCASTING THEIR HISTORY, OPERATION, AND CONTROL (1969) (discussing the history of Japanese broadcast technical innovations); see also *The Evolution of TV*, NHK (2002), <http://www.nhk.or.jp/str/aboutstr/evolution-of-tv-en/index-e.html> (English and Japanese).

73. See generally JOEL BRINKLEY, *DEFINING VISION: THE BATTLE FOR THE FUTURE OF TELEVISION*, (1998) (some observers argued that crucial areas of TV R&D in the U.S. were beginning to erode at this time and the NHK Science and Technical Research Laboratories (“STR”) and other Japanese institutions were already coming to be viewed as strong engineering R&D centers for the technology platforms of modern video technologies).

74. See Kenneth D. Springer, *High Definition Television: New World Order of Fortress*

technical incompatibilities between the Japanese MUSE and the NTSC standard also lent impetus to the movement to development a North American HDTV standard.

In 1982, diverse broadcast industry interests came together to form the Advanced Television Systems Committee ("ATSC") to develop a voluntary standard for an advanced television system to replace the aging North American NTSC television standard.<sup>75</sup> The ATSC initially urged adoption of the MUSE standard, but other U.S. broadcast interests opposed its incompatibility with the NTSC standard, which would require changes to channel allotments and pose other technical difficulties. The International Radio Consultative Committee ("CCIR"),<sup>76</sup> driven by European protectionist concerns,<sup>77</sup> declined to adopt MUSE as a standard, closing the book on the possibility of MUSE becoming an internationally recognized standard for HDTV.

Tandem to industry's growing interest in an advanced successor to NTSC, the FCC was exploring options to satisfy demand for spectrum with physical properties suitable for terrestrial radio users such as public safety (police and emergency services users) and delivery and dispatch companies. Having identified unused portions of the allocated broadcast bands as potential space for new users, the FCC issued a notice seeking comment on opportunities for further sharing between the private land mobile services and the UHF television broadcast service.<sup>78</sup> In its proposal, the FCC described its goal of making additional spectrum available to land mobile services in areas where it was most needed, with minimal impact on television broadcast service. Broadcasters showed significant interest in the proceeding, declaring strong intentions to use the frequencies identified for use with advanced television technologies.<sup>79</sup>

*U.S.A.?*, 24 LAW & POL'Y INT'L BUS. 1309, 1323 (1993).

75. The ATSC was formed out of another industry group, the Joint Committee on InterSociety Coordination ("JCIC"), composed of the Electronic Industries Association, the Institute of Electrical and Electronics Engineers, the National Association of Broadcasters, the National Cable Television Association, and the Society of Motion Picture and Television Engineers. See *Advanced Television Systems and Their Impact Upon the Existing Television Broad. Service., Fourth Report & Order*, 11 FCC Rcd. 17,771 (1996) [hereinafter *ATS 4th*].

76. The International Radio Consultative Committee (CCIR, from the French acronym), a section of the United Nations' International Telecommunications Union, advises on spectrum allocations and communications standards.

77. See LAURA D'ANDREA TYSON, *WHO'S BASHING WHOM: TRADE CONFLICT IN HIGH-TECHNOLOGY INDUSTRIES* 240 (1991).

78. See *Further Sharing of the UHF Television Band by Private Land Mobile Radio Services, Notice of Proposed Rule Making*, 101 F.C.C.2d 852 (1985) (the proceeding was opened in response to various petitions and after a 1983 report by the FCC's Office of Science and Technology) [hereinafter *Further Sharing of the UHF*]. See also VICTOR TAWIL, *ANALYSIS OF TECHNICAL POSSIBILITIES FOR FURTHER SHARING OF THE UHF TELEVISION BAND BY THE LAND MOBILE SERVICES IN THE TOP TEN LAND MOBILE MARKETS* (1983).

79. In his concurring statement, Commissioner Henry Rivera stated that the action could

The pace of the march toward HDTV quickened in July 1987, when the FCC issued its First Notice of Inquiry on Advanced Television Service ("ATS") and formed the Advisory Committee on Advanced Television Service ("ACATS") to review the technical issues and provide a recommendation for a new ATS standard.<sup>80</sup> Momentum for a new standard further accelerated with the first congressional hearing on HDTV, held in October 1987, and the ACATS call for an open competition for development of the best ATS proposal. The Japanese analog-based MUSE standard was an early leader in these trials until 1990, when the FCC (on seeing a demonstration of the feasibility of a digital TV solution) declared that the new ATS standard would have to support a genuine HDTV signal at least twice the resolution of existing television images and be capable of being "simulcast" on different channels.

ACATS and the ATSC began collaborating on a recommendation for technical specifications for ATS. With a decision in early 1993 that a digital standard would be superior to an analog one, several former ATV competitors formed a "Grand Alliance" in May 1993 to collaborate on a single standard incorporating the best features of each system.<sup>81</sup> In November 1995, the ACATS recommended the Grand Alliance prototype DTV standard, which the FCC formally proposed in May 1995 as the new terrestrial broadcasting ATS standard.<sup>82</sup> The FCC adopted it with some modifications in December 1996.<sup>83</sup>

The ATSC standard for DTV represented a significant enhancement to the aging NTSC standard and held numerous benefits for broadcast stations transitioning to digital.<sup>84</sup> Digital techniques for encoding and decoding broadcasts offer improvement of the quality of reception and resilience to interference. Under the new standard, station management

stifle the potential of the low-power TV ("LPTV") service and argued that insufficient time had been afforded to determine the service's spectrum needs. *See* Further Sharing of the UHF, *supra* note 78 (concurring Statement of Commissioner Henry Rivera).

80. Advanced Television Systems and Their Impact on the Existing Television Broadcast Service, *Notice of Inquiry*, 2 FCC Rcd. 5125 (1987).

81. Grand Alliance was formed with the participation of AT&T (now Lucent Technologies), David Sarnoff Research Center, General Instrument Corporation, Massachusetts Institute of Technology, Philips Electronics North American Corporation, Thomson Consumer Electronics and Zenith Electronics Corporation. ATS 4th, *supra* note 75 at 17774, ¶ 4 n.10.

82. Advanced Television Systems and Their Impact Upon the Existing Television Broad. Service, *Fifth Further Notice of Proposed Rulemaking*, 11 FCC Rcd. 6235 (1996) (proposing ATSC as the DTV standard).

83. ATS 4th, *supra* note 75 (adopting ATSC as the new DTV standard).

84. RICHARD M. NUNNO, SCIENCE POLICY RESEARCH DIV., TELECOMMUNICATIONS SIGNAL TRANSMISSION: ANALOG VS. DIGITAL (1996) (discussing the differences between NTSC and ATSC standards); *see generally* MICHAEL SILBERGLEID & MARK PESCATORE, THE GUIDE TO DIGITAL TELEVISION (2d ed. 1999) (discussing the technical advantages of digital television technology).

can select actual channels flexibly while presenting users with a stable set of “virtual channels.” Thus, management can change the actual frequency of “channel 2” without the consumer ever needing to adjust the tuning of the television set.<sup>85</sup> Multicasting, also enabled by the ATSC standard, allows station management to offer several channels of digital programming simultaneously using the same amount of spectrum formerly required for one analog program. Some stations took advantage of multicasting to affiliate with more than one network. ATSC also allows the carriage of diverse kinds of video, such as standard definition and high-definition video. However, the many benefits come with a transition cost. As was the case with early UHF television, consumers using an older NTSC receiver had to procure a “digital converter box” and possibly a new antenna to continue to use the television set after the DTV transition.<sup>86</sup>

### *B. The Long, Slow March toward Transition*

With the ATSC standard in place by the end of 1996, the pieces were in place for the FCC to reallocate broadcast spectrum among existing broadcast and new, non-broadcast users and to establish a deadline for stations to cease analog broadcasts and relinquish their licenses to excess spectrum.

#### 1. Changes in Power Requirements and Spectrum Allocation

##### *a. Existing License Holders*

In 1997, the FCC adopted a DTV Table of Allotments that employed a “service replication/maximization” approach to provide existing broadcasters with DTV channel and power assignments that would replicate the quality and geographic area covered by their existing NTSC analog license.<sup>87</sup> The FCC calculated the power necessary to replicate a station’s existing analog grade B broadcast contour with a

---

85. See THE ADVANCED TELEVISION SYS. COMM., INC., ATSC STANDARD: PROGRAM AND SYSTEM INFORMATION PROTOCOL FOR TERRESTRIAL BROADCAST AND CABLE (PSIP) (2009) (containing more details on the Virtual Channel Table).

86. While new TV receivers sold after 2007 were required to include an ATSC tuner if an NTSC tuner was installed, the requirements were phased in gradually over the decade and admitted the possible need for the owner of an HD receiver to purchase a converter box or tuner to watch TV post-transition. See ACRA, 47 U.S.C. § 303(s) (1962) (implemented by 47 C.F.R. 15.115(c) (1989) and 47 C.F.R. 15.117(b) (1989)).

87. Advanced Television Systems and Their Impact Upon the Existing Television Broad. Service, *Sixth Report & Order*, 12 FCC Rcd. 14,588 ¶ 12 (1997) [hereinafter *ATS 6th*]; see also 47 C.F.R. § 73.622 (1997) (the table of channel allotments was released as appendix B to the Order).

DTV signal.<sup>88</sup> In its power calculations, the FCC attempted to balance the need to allow stations to compete effectively in the provision of DTV services while minimizing interference between stations and other services.<sup>89</sup> Each eligible full-power broadcaster was provided a second channel to broadcast DTV during the interim until the transition was completed, when broadcasters were required to relinquish one of the channels and return to broadcasting on a single 6 MHz channel.<sup>90</sup> The intent was for broadcasters to be “made whole” by the replication of their existing analog service characteristics on their post-transition channel, which viewers could continue to identify as the original TV channel number using “virtual channels.”

While one of the goals of the DTV transition was to replicate the pre-transition environment for broadcasters, the FCC noted that some broadcasters’ post-transition channels would differ entirely from either their original NTSC analog channel or their interim second DTV channel.<sup>91</sup> In fact, the majority of full-power VHF stations would ultimately transition to UHF channels, with quite different propagation properties and power requirements. With stations transitioning to UHF channels, two engineering considerations became relevant for the power levels allowed by the FCC. For stations moving from a VHF channel to

---

88. NTSC TV broadcast coverage areas are defined by contours that define different levels of expected reception quality. *See generally*, R.A. O’Connor, *Understanding Television’s Grade A and Grade B Service Contours*, BC-14 IEEE TRANSACTIONS ON BROAD. 137-143 (Dec. 1968).

89. ATS 6th, *supra* note 87, at 14,605 ¶ 30 (because broadcasting on the same channel in geographic proximity to another broadcaster can result in interference, from the beginning of broadcast regulation, the need to divide television channel licenses into geographic “markets” was prompted by concerns about interference).

90. *See* 47 U.S.C. § 336(c) (2000) (requiring “that either the additional license or the original license held by the licensee be surrendered to the Commission”); *see also* Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service, *Fifth Report & Order*, 12 FCC Rcd, 12,809, 12,849-50 ¶ 97, 12,815 ¶ 13 [hereinafter ATS 5th]. The additional channel for DTV operations was only made available to existing broadcasters. *See* 47 U.S.C. § 336(a)(1) (2000); *see also* Budget Act of 1997, Pub. L. No. 105-33, § 3003, 11 Stat. 251, 265 (1997) (adding new 47 U.S.C. § 337(e)(1) of the Communications Act) (directing that stations “may not operate at that frequency after the date on which the digital television transition period terminates, as determined by the Commission.”).

91. The FCC considered all core 2-51 channels as fungible. Advanced Television Systems and Their Impact Upon the Existing Television Broadcast Service, *Memorandum Opinion & Order on Reconsideration of the Fifth Report & Order*, 13 FCC Rcd. 6860, ¶ 16 (1998). Nevertheless, the FCC expressed its willingness to permit broadcasters to switch DTV services to an existing NTSC channel at the end of the transition, when feasible. *See* ATS 6th, *supra* note 82 at 14,628 ¶ 84. Moreover, the FCC created its allotments to ensure service area “replication” by matching a station with a channel that best replicated the existing service areas, but did allow stations flexibility in providing service within these new service areas. *See* ATS 6th, *supra* note 87 at 14,630 ¶ 90. As discussed in more detail below, many stations in fact did not reach 100 percent coverage of their prior analog services areas.

a UHF channel, higher power levels were necessary to replicate the original NTSC analog coverage area, given the general rule that higher frequencies require greater power to provide equivalent coverage.<sup>92</sup> On the other hand, error correction and other features of the DTV standard allowed the setting of lower power levels than those required for an equivalent NTSC signal.<sup>93</sup> The latter consideration predominated in most cases so that more stations saw their power requirements fall than rise.<sup>94</sup>

*b. Reallocations and New Users*

Another factor that influenced the selection of transitioning stations' channels was found in the other primary goal of the DTV transition—that of reallocating some broadcast spectrum for other uses. The Budget Act of 1997 required the FCC to reallocate 24 megahertz of spectrum in the UHF channels 60–69<sup>95</sup> for public safety services by January 1, 1998, and to make the remaining 36 megahertz of the band available for commercial use via competitive bidding (i.e., a spectrum auction) after January 1, 2001.<sup>96</sup> The FCC reallocated TV channels 63–64 and 68–69<sup>97</sup> to public safety radio services such as emergency dispatch.<sup>98</sup> The FCC reallocated TV channels 60–62 and 65–67<sup>99</sup> for fixed and mobile telecommunications and broadcasting, with the licenses to be assigned by competitive bidding. In addition, the FCC reallocated

---

92. The FCC used procedures and techniques discussed in the Office of Engineering and Technologies Bulletin No. 69 in determining the appropriate power levels and in general discuss the phenomenon as the “dipole effect” defined for low-VHF, high-VHF, and UHF. *See* FED. COMM'N COMM'N, LONGLEY-RICE METHODOLOGY FOR EVALUATING TV COVERAGE AND INTERFERENCE (2004). The Longley-Rice technique is widely used for predicting the geographic coverage of a radio system under certain conditions. *See* G.A. HUFFORD ET AL., U.S. DEPT OF COMMERCE, A GUIDE TO THE USE OF THE ITS IRREGULAR TERRAIN MODEL IN THE AREA PREDICTION MODE (1982) (describing the software and modeling techniques used by the FCC for the Longley-Rice point-to-point radio propagation model); *see also* Letter from G.A. Hufford to users of the model, (Jan. 30, 1985) (identifying modifications to the computer program).

93. Power levels were ultimately reduced less than was originally thought would be the case as field trials informed the engineering analysis.

94. *See infra* Part III.A.

95. These channels are the 746–806 MHz band.

96. 47 U.S.C. § 309(j) (1997).

97. These channels are the 764–776 MHz and 794–806 MHz bands, respectively.

98. *See* Reallocation of Television Channels 60–69, the 746–806 MHz Band, 12 FCC Rcd. 22,953 (1998). As discussed briefly above, the FCC allocates spectrum on the basis of services such as for fixed or mobile use by public safety users regulated by FCC Rules in Part 90. In addition, the FCC regulates users of some services in some bands on the basis of a priority of rights to protection as “primary” or “secondary” users. *See* 47 C.F.R. § 2.106 (2010) (Table of Allocations).

99. These channels are the 746–764 MHz and 776–794 MHz bands, respectively.

other spectrum, reducing the amount of spectrum devoted to television broadcast to a core spectrum of channels 2-51 after the end of the transition,<sup>100</sup> making channels 52-69 (totaling 108 MHz of spectrum) available for new uses.<sup>101</sup> The spectrum made available from these reallocations was highly sought after because of its valuable propagation characteristics.<sup>102</sup>

As discussed in more detail below, television broadcast use of channels outside the core spectrum was originally to be ended after May 2003, but the delay of the DTV transition date (ultimately to June 2009) by changes to the statute also delayed making available spectrum intended for public safety and commercial wireless uses. Furthermore, in some geographic areas broadcasters could not “move in” to their new spectrum until other stations “vacated the premises.” In some cases, complicated cascading scenarios of stations vacating channels to be used by other users may have influenced broadcasters’ decisions regarding when to turn off analog NTSC channels.

## 2. The Mandatory Transition to DTV and Cessation of Analog Broadcasting

Congress and the FCC took steps to ensure that consumers would enjoy the benefits of DTV by adopting policies that encouraged and eventually required manufacturers and broadcasters to transition to the new standard. The policies encouraging compliance included the opportunities for broadcasters to develop temporary DTV operations on separate channels that were described in the previous section. However, achieving the ultimate goal of transitioning all broadcasting to the new DTV standard, and the concomitant freeing of broadcast spectrum for new uses, proved challenging. In this section, we review the legislative

100. See Reallocation & Service Rules for 698-746 MHz Spectrum Band (Television Channels 52-59), GN Dkt. No. 01-74, *Report & Order*, 17 FCC Rcd. 1022, 1023 ¶ 1 (2002) (discussing the Commission’s core channel policy for channels 2-51). “The ‘core spectrum’ included the low-VHF channels 2 to 4 (54-72 MHz) and 5 to 6 (76-88 MHz), VHF channels 7 to 13 (174-216 MHz) and UHF channels 14-51 (470-698 MHz), but does not include TV channel 37 (608-614 MHz), which is used for radio astronomy research.” Third Periodic Review of the Commission’s Rules and Policies Affecting the Conversion To Digital Television, *Notice of Proposed Rulemaking*, 23 F.C.C.R. 2994, 3001 n.20 (2007). In order to protect sensitive radio astronomy operations, use of TV channel 37 was not allowed for NTSC or DTV service. See DTV Sixth Memorandum Opinion & Order, 13 FCC Rcd. at 7419 ¶ 5; see also Numerical Designation of Television Channels, 47 C.F.R. § 73.603(c) (2010).

101. Channels 52-59 were reallocated for new wireless services in 2001. See Reallocation and Service Rules for the 698-746 MHz Spectrum Band (Television Channels 52-59), *Report & Order*, 17 FCC Rcd. 1022, 1024 (2002).

102. U.S. GOV’T ACCOUNTABILITY OFFICE, DIGITAL TELEVISION TRANSITION: ISSUES RELATED TO AN INFORMATION CAMPAIGN REGARDING THE TRANSITION 49 (2005).

history that structured the DTV transition and the FCC regulations that specifically instructed stations how and when to transition.

*a. Legislative History of the DTV Transition*

Congress, in the Telecommunications Act of 1996, undertook the most significant revision of communications law since the establishment of the FCC.<sup>103</sup> In the section of the Act pertaining to broadcasting, Congress directed the FCC to provide new licenses (at no cost) to incumbent broadcasters for the provision of DTV broadcasting under the condition that broadcasters would have to return either the new or original analog license at some date. The FCC issued some 1,600 licenses<sup>104</sup> and adopted mandatory dates that stations would have to “transition” to DTV broadcasting.<sup>105</sup> The deadlines depended on the size of the markets where the stations were located. Stations in the top 10 markets would have to transition by May 1, 1999; those in markets 11–30 by November 11, 1999; all other full-power commercial stations by May 1, 2002; and noncommercial stations by May 1, 2003. However, the FCC decided stations would not have to relinquish one of their channels and cease analog broadcasting until 2006.<sup>106</sup>

In the first of many modifications to and delays of the transition scheme, Congress revisited the issue in the Balanced Budget Act of 1997.<sup>107</sup> While the Act made statutory the regulatory requirement to cease analog broadcasting by the end of 2006, it relaxed the transition dates listed above by making “extensions” available. If 85 percent of households in any given market either did not have DTV-ready receivers or were subscribers of cable or satellite, the deadlines would not apply and the DTV transition in that market would not proceed.<sup>108</sup>

The distribution of licenses to existing licensees proceeded after an

103. Telecommunications Act of 1996, Pub. L. No. 104, 110 Stat. 56 (1996) (adding §336 to the Communications Act of 1934).

104. The DTV spectrum that was given to broadcasters had an estimated value of between \$11 billion and \$70 billion. The 104th Congress debated whether to require the FCC to auction the DTV licenses, but in the end granted no authority to the FCC to auction the spectrum. LENNARD G. KRUGER, *DIGITAL TELEVISION: AN OVERVIEW* 4 (Susan Boriotti & Donna Dennis eds., 2002).

105. ATIS 5th, *supra* note 90, at 12,840–12,841 ¶ 76.

106. *Id.* ¶ 99. The FCC intention to require stations to cease analog broadcasting in 2006 was made statutory by the Balanced Budget Act of 1997, codified in various section of 42 U.S.C.

107. *See* Balanced Budget Act of 1997.

108. 47 U.S.C. § 309(j) (1997). There were other conditions as well: if one or more of the television stations affiliated with the four national networks are not broadcasting a digital television signal; or if digital-to-analog converter technology is not generally available in the market of the licensee.

unprecedented engineering effort at the FCC that required a careful selection of channel allotments at precise power levels in each geographic market to prevent interference to non-broadcast services and broadcast stations alike. Many DTV licenses allotted spectrum in the UHF band, where higher power levels were necessary to maintain the equivalent service areas to the existing analog broadcast footprint.

In 2001, FCC Chairman Michael Powell formed the DTV Task Force to track and facilitate early progress of DTV adoption. Early preparations for the transition indicated signs of concern. In the Dallas-Fort Worth area, tests by station WFAA with DTV in 1998 resulted in interference to 12 heart monitors at the Baylor University Medical Center. Additionally, stations complained of the significant cost of the transition. By 2002, about three-quarters of the 1,240 full-power broadcast stations had failed to meet their DTV construction requirements.<sup>109</sup> Stations complained of a variety of difficulties. Foremost among their concerns were difficulties acquiring approvals by local governments of new antenna towers and lack of funding for new facilities.

As 2006 approached, along with the date for relinquishing analog broadcast spectrum set in the Balanced Budget Act of 1997, Congress became increasingly concerned that the 85 percent “readiness” threshold would be met in few markets, preventing a timely transition. By 2005, only 3.3 percent of television households were capable of receiving DTV signals.<sup>110</sup> Debate began anew in Congress, not simply on extending the previous deadline but instead focusing on adopting a new “hard” date that would not be subject to extensions or delays. In February 2006, the Deficit Reduction Act of 2005<sup>111</sup> set the first so-called “hard deadline,” directing that the FCC terminate all analog television licenses by February 18, 2009.<sup>112</sup> Thus, February 17, 2009 was to be the final day of analog television broadcasting in the U.S.

Entering 2008, concerns arose in Congress again regarding the public’s preparedness for the February 17, 2009 transition. In its report in

109. GEN. ACCOUNTING OFFICE, TELECOMMUNICATIONS: MANY BROADCASTERS WILL NOT MEET MAY 2002 DIGITAL TELEVISION DEADLINE 27 (2002).

110. See Evan Kwerel & Jonathan Levy, *The DTV Transition in the US*, in DIGITAL BROADCASTING: POLICY AND PRACTICE IN THE AMERICAS, EUROPE AND JAPAN 32 (Martin Cave & Kiyoshi Nakamura eds., 2002).

111. Digital Television Transition and Public Safety Act of 2005 (“DTV Act”), Pub. L. No. 109-171, §§3001-3013, 120 Stat. 4, 21-28 (2006) (Title III of the Deficit Reduction Act of 2005, Pub. L. No. 109-171, 120 Stat. 4 (2006) (“DRA”)) (codified as amended at 47 U.S.C. §§ 309(j)(14) and 337(e)) (amending §309(j)(14) of the Communications Act to establish February 17, 2009 as the hard deadline for termination of analog transmissions by full-power stations).

112. See 47 U.S.C. 309(j)(14) (2006).

November 2007, the Government Accountability Office concluded that no comprehensive plan or strategy to measure progress and results in the transition existed in the federal government, and that consumer outreach efforts were being conducted primarily by private sector stakeholders on a voluntary basis.<sup>113</sup> As the nation entered the final months before the February deadline, Congress and President Obama's concerns about the NTIA's coupon program for DTV converter boxes<sup>114</sup> and general lack of preparedness of consumers grew. In response, the DTV Delay Act was signed into law a week before the erstwhile deadline.<sup>115</sup> The new deadline provided by the Act (and this time the final deadline) was June 12, 2009.

### *b. FCC Rules for Transitioning*

From a regulatory perspective, the DTV transition was more complex than merely giving deadlines to broadcasters. Since some stations wished to cease analog broadcasting before the deadline, the FCC promulgated rules to allow the transition to proceed smoothly, without unduly hindering stations or creating confusion among consumers.<sup>116</sup>

#### 1. Voluntary Early Transition

In December 2007, in a report and order on DTV matters ("Third Review R&O"), the FCC adopted rules allowing stations to transition in

113. GEN. ACCOUNTING OFFICE, TELECOMMUNICATIONS: INCREASED FEDERAL PLANNING AND RISK MANAGEMENT COULD FURTHER FACILITATE THE DTV TRANSITION (Nov. 2007).

114. The Department of Commerce's National Telecommunications and Information Administration ("NTIA") administered the TV Converter Box Coupon Program authorized in the Digital Television Transition and Public Safety Act of 2005, § 3005 (2006). Households were eligible to receive two \$40 "coupons" good towards the purchase of qualifying digital converter boxes. During the weeks leading up to the transition significant numbers of consumers were on a waitlist to receive coupons while expired coupons funds were recommitted and the overall total funding for the program neared exhaustion. *See generally Digital TV Transition and Public Safety; TV Converter Box Coupon Program*, NTIA, <http://www.ntia.doc.gov/dtvcoupon/> (last visited Apr. 10, 2011).

115. DTV Delay Act, Pub. L. No. 111-4, 123 Stat. 112 (2009) (47 U.S.C. § 609); *see also Implementation of the DTV Delay Act, Report & Order & Sua Sponte Order on Reconsideration*, 24 FCC Rcd. 1607 (2009); Press Release, President Barack Obama, Statement of President Barack Obama on Signing the DTV Bill (Feb. 11, 2009), *available at* [http://www.whitehouse.gov/the\\_press\\_office/StatementofPresidentBarackObamaonSigningtheDTVBill/](http://www.whitehouse.gov/the_press_office/StatementofPresidentBarackObamaonSigningtheDTVBill/).

116. The FCC also set rules for the television receiver equipment market, mandating that all devices intended for video reception (e.g., TVs and digital video recorders) manufactured after March 1, 2007, include an ATSC tuner. Certain categories of televisions had even earlier deadlines.

advance of the February 17, 2009 deadline then in effect.<sup>117</sup> The procedures allowed early termination of analog service, provided the change would facilitate certain goals of the transition. The procedures outlined eligibility requirements, required showings to the Commission, and requirements to inform viewers for early terminations prior to the last 30 days before the deadline. After the DTV Delay Act changed the transition date from February 17, 2009 to June 12, 2009, the same rules applied to the new deadline (with some modifications). The procedures for early termination vary slightly depending on the service, but most importantly, they vary on *when* the change would occur.

## 2. Early Termination Prior to November 19, 2008

The Third Review R&O outlined rules for different service scenarios. One set of rules related to the termination or reduction of the existing analog NTSC service, and, in effect, governed the early DTV transition of a station.<sup>118</sup> The procedures for analog termination are similar to the sets of rules for the other service changes, such as terminating ATSC service on the temporary DTV channel.<sup>119</sup> The first requirement is that stations must obtain approval from the FCC before making changes. Requests had to be filed 90 days in advance of the planned termination, and stations had to show that:

- (1)The analog service reduction or termination was directly related to the construction and operation of its, or another station's, post-transition facilities; and<sup>120</sup>
- (2)The station planned to notify viewers on its analog channel about

---

117. See Third Review R&O, *supra* note 1, at 2995-2996.

118. *Id.* at 3045 ¶ 107.

119. As part of an early transition, stations terminating their analog and commencing DTV service on their analog channel or moving to a new channel for post-transition operations were also allowed to terminate existing digital service on their pre-transition DTV channels prior to the transition date.

120. Examples identified as "directly related" to the construction and operation of post-transition facilities included: "(1) Stations that need to reposition their digital and analog antennas before the end of the transition; (2) Stations that need to add a third antenna to their tower but cannot do so without reducing or terminating analog service because the tower cannot support the weight of the additional transmission facilities; (3) Stations on a collocated tower that must coordinate a reduction or termination with other stations in order to configure their final, post-transition facilities; (4) Stations with equipment currently in use with their analog operations that they plan to use with their digital operations; and (5) Stations that must terminate operation on their analog channel in order to permit another station to construct its post-transition DTV facilities on that channel." Third Review R&O, *supra* note 1, at 3045 ¶ 116.

the planned changes and inform them about how they can continue to receive the station.<sup>121</sup>

Appropriate notification of viewers of impending changes was an important component of the early termination procedures.<sup>122</sup> Notification was required to commence no fewer than 60 days prior to termination of the analog signal.<sup>123</sup>

The procedures also allowed most stations with an out-of-core DTV channel “to terminate pre-transition digital service and transition directly from their analog to their post-transition digital channel (*i.e.*, ‘flash cut’ approval)[,]”<sup>124</sup> and to move digital channels to new channels.<sup>125</sup> The FCC viewed these early transitions favorably, identifying that they could facilitate the transition by freeing engineering, construction, and spectrum resources for those stations building later. Thus, early terminations were seen to advance the transition by setting in motion “daisy-chains” of early transitions, wherein as channels were vacated by a departing station they freed up space in the spectrum for an incoming station.

### 3. Early Termination from November 19, 2008 through February 16, 2009

The FCC provided streamlined notification procedures for stations terminating analog or digital broadcasting within 90 days of the February 17, 2009 transition date (*i.e.*, beginning on or after November 19, 2008). The procedures required stations to file notification with the Commission 30 days in advance of the planned service reduction or termination. The station had to show that the change in service was necessary for purposes of the transition. The station also had to notify its

---

121. Notifications were required “every day on-air at least four times a day including at least once in primetime for the 60-day period prior to the planned service reduction or termination. These notifications must include: (1) the station’s call sign and community of license; (2) the fact that the station is planning to or has reduced or terminated its analog or digital operations before the transition date; (3) the date of the planned reduction or termination; (4) what viewers can do to continue to receive the station, *i.e.*, how and when the station’s digital (5) information about the availability of digital- to-analog converter boxes in their service area; and (6) the street address, email address (if available), and phone number of the station where viewers may register comments or request information.” *Id.* at 3045 ¶ 117.

122. *Id.*

123. *Id.* ¶ 114.

124. *Id.* ¶ 124.

125. *Id.* ¶ 121 (allowing moving from a pre-transition DTV channel to a post-transition channel, provided: “(1) The early transitioning station must not cause impermissible interference to another station; and (2) The early transitioning station must continue to serve its existing viewers for the remainder of the transition and commence its full, authorized post-transition operations on February 18, 2009.” This date marks the expiration of the transition deadline.).

viewers on pre-transition channels about the planned service change and tell consumers how they could continue to receive the station. The FCC did not require prior approval (as it had before).

#### 4. Early Termination on February 17, 2009

The DTV Delay Act provided that stations that sought to terminate their analog service before the new June 12, 2009 deadline would be subject to the FCC's existing rules for early termination of analog service.<sup>126</sup> Given that until the Act was passed a week before the erstwhile deadline stations were preparing to transition on February 17, 2009, the FCC waived generally the early termination requirements outline above for stations wishing to terminate on that day.<sup>127</sup> Stations were not required to submit pleadings or engineering data in support of requests to terminate analog service on February 17, 2009. Thus, stations that intended to transition and had incentive to do so were generally permitted to transition on the February 17, 2009 date. We discuss exceptions to this in section III.B. About one-quarter of stations transitioned on this date, as we discuss in the empirical section below.

#### 5. Early Termination after February 17, 2009

After the DTV Delay Act postponed the mandatory analog shutoff date from February to June, stations that sought to transition after February 17, 2009 were subject to the existing rules for early termination. In particular, an early termination 90 days prior to June 12, 2009 did not require FCC approval, but requests to terminate between February 18 and March 13 required advance approval and filings showing need. With no option to waive these requirements, stations effectively entered a *de*

---

126. DTV Delay Act, *supra* note 115 at § 4(a) (2009) (“Permissive Early Termination Under Existing Requirements—Nothing in this Act is intended to prevent a licensee of a television broadcast station from terminating the broadcasting of such station’s analog television signal (and continuing to broadcast exclusively in the digital television service) prior to the date established by law under section 3002(b) of the Digital Television Transition and Public Safety Act of 2005 for termination of all licenses for full-power television stations in the analog television service (as amended by section 2 of this Act) so long as such prior termination is conducted in accordance with the Federal Communications Commission’s requirements in effect on the date of enactment of this Act, including the flexible procedures established in the Matter of Third Periodic Review of the Commission’s Rules and Policies Affecting the Conversion to Digital Television (FCC 07–228, MB Docket No. 07–91, released December 31, 2007)”).

127. FCC Announces Procedures Regarding Termination of Analog Television Service On or After February 17, 2009, *Public Notice*, 24 FCC Rcd. 1586 (2009), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-09-6A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-6A1.pdf).

*facto* cooling off period immediately after the transition, with no stations transitioning between February 18 and March 13.

As of March 14, 2009 (90 days before the new statutory transition deadline), the streamlined notification procedures were again available to broadcasters. For stations terminating analog on or after March 14, the FCC required at least 30 days prior notification of the termination date and viewer notification at least 30 days prior to the termination of analog service. However, stations transitioning after February 17, 2009 were subject to a number of additional public interest obligations.

Affiliates of the major networks—ABC, CBS, Fox, and NBC—that wished to terminate analog service prior to June 12 were required to ensure that at least 90 percent of their analog viewers would continue to receive analog service from another major network affiliate through June 12. While the service could consist of continuing regular analog programming from one or more of the major network affiliates remaining on the air until the transition, service was also possible from an “enhanced nightlight” service making available (in analog) news, public affairs and emergency information from a major network affiliate. The Short-term Analog Flash and Emergency Readiness Act (“Analog Nightlight Act”)<sup>128</sup> required the Commission to develop and implement a voluntary program to “encourage and permit” analog television service for a 30-day period after the DTV transition for viewers who had not successfully transitioned by the deadline.<sup>129</sup> This voluntary program became required after the delay, except for noncommercial stations experiencing significant financial hardship that were allowed to terminate analog service beginning on March 27.

### III. STRATEGIC CONCERNS OF THE DTV TRANSITION

As the history of the legislative and regulatory action in the previous section documents, television broadcasters faced many choices of when to transition fully to DTV and turn off their analog transmissions. Like any business decision, the stations considered the costs and benefits of the various dates they were allowed to transition. This section reviews some of the primary factors influencing the stations' decisions.

---

128. Short-term Analog Flash and Emergency Readiness Act, Pub. L. No.110-459, 122 Stat. 5121 (2008).

129. The Analog Nightlight Act was enacted on December 23, 2008, prior to the enactment of the DTV Delay Act, which changed the nationwide transition deadline from February 17 to June 12, 2009.

### A. *The Costs of the Transition for Stations*

The two major cost considerations for a station contemplating the DTV transition are the cost of the new equipment necessary to begin digital broadcasting and the power savings from the cessation of analog transmission. All along, many stations complained about the high equipment costs of the transition. In 1999, Station KSTP-TV of Minneapolis-St. Paul reported spending about \$1.5 million to upgrade its facilities for the transition,<sup>130</sup> religious network TBN spent \$5 million upgrading its facilities in New York.<sup>131</sup> Some estimates placed the total costs of upgrading for the transition at around \$1.7 billion for public television stations alone, which is greater than the annual income of such stations.<sup>132</sup>

On the plus side of a station's ledger are the lower electricity bills for broadcasting. As mentioned in section III.B.1.a. above, the switch to DTV had the potential to lower the power requirements needed for broadcasting. Our analysis of the station engineering data filed with the FCC indicates that the input power savings for DTV transmission over analog broadcasting was over five kilowatts ("KW") for the average station.<sup>133</sup> Since by February 2009 stations had already begun DTV broadcasting, the relevant short-run power savings from completing the transition came from terminating analog broadcasting. Shutting down the analog transmission saved an estimated 40.3 KW of power for the average station, for an estimated reduction of about \$2,500 in the monthly energy bill.<sup>134</sup> Thus, by switching, stations could realize savings estimated to be perhaps several thousand dollars per month or more.<sup>135</sup>

130. ROGER L. SADLER, *ELECTRONIC MEDIA LAW* 96 (2005).

131. See George Winslow, *TBN Finishes HD Upgrade in Dallas*, MULTICHANNEL NEWS (May 13, 2009), [http://www.multichannel.com/article/232375-TBN\\_Finishes\\_HD\\_Upgrade\\_in\\_Dallas.php](http://www.multichannel.com/article/232375-TBN_Finishes_HD_Upgrade_in_Dallas.php).

132. See *Current Briefing: Digital Television and Public Television*, CURRENT.ORG, <http://www.current.org/dtv/> (last visited Mar. 2, 2010).

133. The average value of the difference in our estimate of the input power necessary for the analog and digital broadcasts of a station in our data is 5.6 KW (see Table 2). See also *infra* note 159.

134. Assuming a station broadcasts an average of 22 hours a day for 30 days, and buys power at the state average commercial retail electricity price (data from 1Q2009), the average savings from turning off analog transmission is estimated from our data to be \$2,575/month. This calculation does not include ancillary electrical costs of operating the transmitter such as de-icing equipment for the antenna, liquid chillers for transmission tubes, and environmental cooling (air conditioning) to remove the heat load from the transmitter.

135. Various industry sources provide monthly estimates of electricity cost savings per station ranging from several thousand dollars to \$20,000 and higher. Andrew M. Seder, *WNEP to Keep Analog Signal Going*, AP NEWSWIRE, Feb. 19, 2009; 2 *Local Stations Plan to Go Digital* Feb. 17, NEWPORT NEWS DAILY PRESS (Feb. 10, 2009) <http://www.tmcnet.com/usubmit/2009/02/10/3977517.htm>; Jennifer Konfrst, *Why Is IPTV Continuing Analog Broadcasting Past Feb. 17?*, IOWA DTV ANSWERS BLOG (Feb. 9, 2009,

For the PBS network alone, the electricity cost savings for the February to June period were \$22 million, which is the main reason most public television stations cited for transitioning in February.<sup>136</sup>

Many stations cited the high cost of maintaining duplicate analog and digital facilities to justify their requests to terminate the analog transmission. In some cases, engineering concerns prevented the use of the same antennas or other facilities for DTV as for analog broadcasting. In other cases, stations chose to construct separate facilities.<sup>137</sup> Older analog broadcast transmitters can be particularly expensive to maintain, since procuring replacement parts can be difficult, and even routine maintenance can require specialized engineering expertise. The costs of continuing to operate older facilities created an additional business risk when maintaining an analog facility in tandem with an operational DTV facility.

Some costs of the transition were less certain for stations. In an era of declining broadcast viewership, stations were understandably skittish about losing viewers because of unforeseen technical problems or lack of readiness on the part of viewing households.<sup>138</sup> Furthermore, even if all went well with the transition, service footprints were changing in some locations, leading to a loss of some viewers. One study claimed that there would be “significant gaps” in DTV signal coverage across the country, since most consumers were unaware that they would have to add or upgrade their antennas.<sup>139</sup> As explained in section II.C.2 above, a loss of viewers translates into lost advertising dollars for stations, and thus represents a real (if uncertain) consideration for station managers.

5:27 AM), <http://iowadigitaltv.blogspot.com/2009/02/why-is-iptv-continuing-analog.html?showComment=1234230120000>. Conversations with FCC staff indicate that a savings of \$20,000 would likely be extreme.

136. See Dan DiPaolo, *WJAC to Continue Offering Analog Broadcast*, DAILY AMERICAN (Feb. 7, 2009), [http://articles.dailyamerican.com/2009-02-07/news/26296294\\_1\\_analog-broadcasts-coupon-program-converter-boxes](http://articles.dailyamerican.com/2009-02-07/news/26296294_1_analog-broadcasts-coupon-program-converter-boxes).

137. For example, the TBN network stated that “we have a lot of legacy facilities that are aging and dying; and we decided that rather than keeping a limping facility together, we would just start from scratch and go HD from stem to stern.” Winslow, *supra* note 131.

138. See, e.g., Dennis Haarsager, Assoc. Vice President, Educ. & Public Media, Wash. State Univ., Presentation at Broadcasting Management Association Conference: Over-the-Air Strategies 2007-2009 (May 31, 2007) (PowerPoint slides available at <http://www.bloobble.com/broadband-presentations/presentations?itemid=433>) (warning that (at the time) many viewers lacked basic information about the DTV transition and that losing OTA-only viewers could translate to losing one-fifth of PBS members).

139. Press Release, Centris, New Research Sheds Light on Major Glitch in the DTV Transition (Feb. 12, 2008). The Centris study claimed to use a more realistic engineering model of household reception than the FCC was using, and that the results showed that there was little continuous DTV coverage beyond 35 miles from the broadcast antenna.

### B. *Other Strategic Aspects of the Transition*

In the economic models of stations' decision-making developed in the next section, we take the change in electricity costs and the potential to lose viewers as the salient strategic considerations for station managers. Since we consider the stations' decision made right before the erstwhile February deadline, we do not need to consider the stations' expenditure on new or upgraded facilities, since those were already in place. However, a few other factors also may have influenced when stations turned off their analog broadcasts. Two of these are cost sharing and coordination among broadcasters and explicit intervention by the FCC.

The costs of educating consumers about the DTV transition were a concern to broadcast stations. The FCC reported that, in many markets, broadcasters cooperated in funding and operating call centers, walk-in centers, and other consumer-education efforts. In some markets, some stations actively ran the facilities with their own staff, with other broadcasters participating passively in the efforts by providing funding.<sup>140</sup> As another example of cost-sharing, stations in some markets actively coordinated the decision (and in some cases pooled resources) to satisfy the obligation for at least one station to continue analog broadcasting after all other stations switched to DTV.<sup>141</sup> In both examples, a passive firm might weigh an active firm's ability to recoup some value from operating the call center or remaining analog against the costs the firm would incur. We do not explicitly model these considerations.

In some cases, the flurry of regulatory activity in the final few weeks before February 17, 2009, resulted in stations not being able to transition when they wished. Although, as noted above, stations that wished to transition on February 17 were generally allowed to do so, the FCC reserved the right to require a station to continue its analog broadcasts under certain conditions. The FCC specifically stated it would consider such action if it found that most stations in a market were planning to terminate service, and that "the market [was] one in which many viewers [were] unprepared for the transition or at risk if the transition

---

140. In the State of Oregon and in other parts of the country, Public Broadcast stations with existing facilities for handling large call volumes served as the call centers for the entire broadcast market. See generally *Digital TV Transition Happens Today!*, OREGON PUBLIC BROADCASTING (June 12, 2009), [http://www.facebook.com/note.php?note\\_id=91606741957](http://www.facebook.com/note.php?note_id=91606741957) (last visited Feb. 12, 2011).

141. Implementation of Short-Term Analog Flash and Emergency Readiness Act; Establishment of DTV Transition "Analog Nightlight" Program, *Report & Order*, 24 FCC Rcd. 6966 (2009) ("Analog Nightlight Order"). 121 stations were reported to have provided nightlight service in 87 markets after the June 12 transition.

proceed[ed].”<sup>142</sup> As late as February 10, the FCC was still reminding broadcasters that it could yet find some of their plans “contrary to the public interest,”<sup>143</sup> and its decisions were released the next day.<sup>144</sup> As a result, while 26 percent of the stations expressed the desire to transition on February 17, not all of them did so. About 10 percent (43) of the stations wishing to switch off their analog broadcasts on February 17 ultimately chose not to, thus avoiding having to comply with the additional requirements placed upon them if they would have proceeded with the transition.<sup>145</sup> These stations may have deemed some of the extra requirements, such as continuing to operate walk-in consumer information and help centers and providing toll-free engineering support to viewers, to be more expensive than postponing the transition.<sup>146</sup> In the next section, we distinguish between the *desire* to transition early, based on the financial costs and benefits, and the actual *decision* to transition early, complicated by the last-minute regulatory intervention.

### C. *Economic Models of the Transition Decision*

In this section, we present two economic models of the stations' decisions of when to transition to DTV. We consider both decision theoretic and game theoretic models. In both models, we assume a station's management considers its own costs and viewership when deciding to switch early. The game theoretic model, in addition, incorporates strategic thinking on the part of management (hereafter, the “station”). In particular, in the game model, a station also looks to the decisions it expects other stations in its market to make, and considers the impact of the others' decisions on its profit. We test the implications of the models in the empirical work in the following sections.

### D. *Decision Theoretic Model*

For clarity of presentation, we model a local television market with

142. FCC Announces Procedures Regarding Termination of Analog Television Service On or After February 17, 2009, *supra* note 127.

143. FCC Releases Lists of Stations Whose Analog Operations Terminate Before February 17, 2009 or that Intend to Terminate Analog Operations on February 17, 2009, *Public Notice*, 24 FCC Rcd. 1552 (2009), *available at* [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DA-09-221A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-221A1.pdf).

144. FCC Requires Public Interest Conditions for Certain Analog TV Terminations on February 17, 2009, *Public Notice*, 24 FCC Rcd. 1595 (2009).

145. FCC Releases Lists of TV Stations' Responses to Requirements for Analog Termination on February 17, 2009, *Public Notice*, 24 FCC Rcd. 1552, 1553 (2009).

146. *See* FCC Requires Public Interest Conditions for Certain Analog TV Terminations on February 17, 2009, *supra* note 144 (listing the eight measures the FCC required a station in one of the “unprepared” markets to fulfill in order to terminate on February 17, 2009).

only two stations, labeled 1 and 2. Each station is assumed to want to maximize its profit during the transition period, and sets aside the impact of its current actions on profits after the transition period. A station earns profits by selling advertising at rate  $p$  per viewer.<sup>147</sup> Revenue from advertising is  $pq$ , where  $q$  is the station's viewership.<sup>148</sup> A station incurs only fixed costs  $C$  to broadcast in the short run, which are of the form

$$C = F + wx$$

where  $F$  includes labor, rent, capital, and other non-power costs,  $w$  is the price of electricity, and  $x$  is the amount of electricity used, which is a function of technical characteristics of the tower, antenna, and cooling systems used.

The action  $a$  available to each station is to transition early to digital broadcasting and turn off analog on February 17, 2009 (action  $a = D$ ), or to continue analog broadcasting for the time being (action  $a = A$ ). We refer to switching on or before February 17 as switching "early." Viewership may be affected by the decision. If station  $i$  switches to DTV early, assume that there is a chance that something goes wrong with the transition, so that when switching the station loses fraction  $\phi_i$  of the original  $q_i^0$  viewers in expectation.<sup>149</sup> Thus, the risk a station takes from action  $D$  is losing viewers. The benefit for the station of transitioning early is the power savings:  $x_i(A) > x_i(D)$  (that is, it takes less power for station  $i$  to broadcast DTV than in analog). The ad price  $p$ , the price of electricity  $w$ , and the non-power cost  $F$  are invariant with respect to a station's action, the latter because this is a short-run analysis.<sup>150</sup> There is no economic switching cost, since every station was supposed to be ready to switch in February and the FCC required no additional filings to justify switching on February 17.<sup>151</sup> Thus, by the time that the switching decision was to be made, switching costs were already sunk. We leave out the possibility that the superior quality or additional video and audio

147. Broadcast advertising prices within a DMA and daypart are largely proportional to the Nielsen point rating of a show (which measures viewership). Negotiations between advertisers and stations can lead to other prices, which we ignore in the model. We also set aside the fact that  $pq$  varies by daypart.

148. We assume that ad prices per viewer will be unaffected by the transition.

149. To be precise,  $\phi q_i^0$  is the expected value of the number of lost viewers, and so incorporates all known changes in the broadcast footprint due to the transition as well as the probability of losing viewers due to unforeseen problems.

150. We are also assuming that the transition decisions, which needed to be finalized in the space of about a week before February 17, were made without enough time to alter the engineering details of the two options facing the station. In other words, for purposes of our modeling we take  $\phi$  to be exogenously determined.

151. See *supra* Part II.B.2.b.

channels enabled by DTV would increase viewership.

The profit,  $\pi$ , of station  $i$ , given its action  $a_i$ , can therefore be expressed as:

$$\pi_i(a_i) = pq_i(a_i) - C_i(a_i) \quad (1)$$

where

$$C_i(a_i) = F_i + wx_i(a_i) \quad (2)$$

$$q_i(\mathcal{A}) = q_i^0 \quad (3)$$

$$q_i(D) = q_i^0 - \phi_i q_i^0 \quad (4)$$

In equations (1)-(4),  $q_i$  denotes the expected number of viewers for station  $i$  during the transition period. We assume that the stations are risk neutral.

Given the profit function, we can now examine a station's decision to switch to DTV. The expected payoff for station  $i$  is  $\pi_i(\mathcal{A}) = pq_i^0 - C_i(\mathcal{A})$  if it stays analog, or  $\pi_i(D) = p(1 - \phi_i)q_i^0 - C_i(D)$  if it switches to DTV. For convenience, define  $d_i = \phi_i pq_i^0$ , the expected lost revenue from transitioning early, and define  $\Delta_i = w[x_i(\mathcal{A}) - x_i(D)]$ , the cost savings from turning off analog. A station decides to switch early (action  $D$ ) if and only if  $d_i < \Delta_i$ . This condition states that the benefits of transitioning (the cost savings  $\Delta$ ) outweigh the expected costs ( $d$ ). The decision rule for switching to DTV, in the absence of strategic considerations, merely has the firm comparing its own costs and benefits of switching, regardless of the characteristics or expected decisions of the other station.

The empirical implications from the decision model are:

1. A station is more likely to transition early the greater is its  $\Delta$ . This implies that higher energy cost savings from transition make the decision to transition early more likely.
2. A station is more likely to transition early the lower is its  $d$ . This implies that a lower probability of losing viewers and a lower amount of advertising revenue potentially lost make the decision to transition early more likely.

Each statement is to be understood holding other factors constant. We explore these implications in the following empirical sections.

#### IV. GAME THEORETIC MODEL

The game theoretic approach to law and economics emphasizes the interdependency of payoffs in a multiple agent setting—in this case, the

fact that one station's profit depends on the other station's decision.<sup>152</sup> In the game, viewership  $q$  for a station depends on *both* stations' actions. If station  $i$  switches to DTV early when the other station continues its analog broadcasting, the  $\phi_i q_i^0$  viewers leaving the station are picked up by the other station.<sup>153</sup> If both stations stay analog or both switch, there is no change in viewership.

The profit of station  $i$  is now a function of both its and its opponent's actions:

$$\pi(a_i, a_j) = pq_i(a_i, a_j) - C_i(a_i) \tag{5}$$

where

$$q_i(A, A) = q_i(D, D) = q_i^0 \tag{6}$$

$$q_i(A, D) = q_i^0 + \phi_j q_j^0 \tag{7}$$

$$q_i(D, A) = q_i^0 - \phi_i q_i^0 \tag{8}$$

Given the profit functions, we can now examine a station's strategic incentive to switch to DTV. The payoff matrix for station 1 is:

|                    |   | Station 2's Action            |                                    |
|--------------------|---|-------------------------------|------------------------------------|
|                    |   | A                             | D                                  |
| Station 1's profit | A | $pq_1^0 - C_1(A)$             | $p(q_1^0 + \phi_2 q_2^0) - C_1(A)$ |
|                    | D | $p(1 - \phi_1)q_1^0 - C_1(D)$ | $pq_1^0 - C_1(D)$                  |

If station 1 expects that station 2 will choose to stay with analog (action  $A$ ), then (comparing the payoffs to 1 in the first column of the matrix) 1 chooses to switch early (action  $D$ ) if and only if  $d_1 < \Delta_1$ , as in the decision theoretic model. If, instead, station 1 expects that station 2 will choose to switch early (action  $D$ ), then (comparing the payoffs in the second column of the matrix) 1 chooses to also switch early if and only if  $d_2 < \Delta_1$ . If not, then the expected benefits to station 1 of letting station 2

152. See DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW 1 (1994).

153. For simplicity, we assume there is no leakage of viewership to cable or satellite television. Around the time of the transition, industry observers expected few over-the-air viewers to switch to cable or satellite; see Virgil Dickson, *Too Early to Say Whether DTV is Pushing Consumers to DBS*, COMMC'NS DAILY, Mar. 23, 2009, at 8-9. Nielsen estimates that about one-fifth of over-the-air viewers readied for the transition by subscribing to cable; see John Eggerton, *Nielsen: Viewing Rebounds After Early Post-DTV Decline*, BROAD. & CABLE (July 23, 2009), [http://www.broadcastingcable.com/article/316241-Nielsen\\_Viewing\\_Rebounds\\_After\\_Early\\_Post\\_DTV\\_Decline.php](http://www.broadcastingcable.com/article/316241-Nielsen_Viewing_Rebounds_After_Early_Post_DTV_Decline.php). Modifying the model by assuming that a constant fraction of viewers "leak" to cable instead of going to the other station would change none of the predictions of the model.

move first ( $d_2$ ) would outweigh the costs of transitioning and station 1 would stay with analog. In this case, the best response of station 1 is clearly strategic. When the other station is going to switch to DTV, station 1 recognizes that the other stations' viewers at risk are what matters for its decision; if something goes wrong with station 2's transition, some of its viewers will migrate to station 1.

The best responses for station 1 can now be summarized: if station 2 plays  $A$ , play  $D$  if and only if  $d_1 < \Delta_1$ ; if station 2 plays  $D$ , play  $D$  if and only if  $d_2 < \Delta_1$ . The decision facing station 2 involves the same considerations and results in a similar set of best responses. While one can proceed to find the Nash equilibrium of the game,<sup>154</sup> the best responses already furnish us with the implications we wish to test. Note that implications 1 and 2 from the decision theoretic model also apply to the game theoretic model. The game provides an additional implication not found in the previous model:

3. When its rival switches to DTV, a station is more likely to transition early the greater the difference between its  $\Delta$  and its rival's  $d$ . This implies that a lower expected number of the *rival's* viewers potentially gained (or the lower the value of the advertising revenue from those viewers) make the decision to transition early more likely.

## V. EMPIRICAL EXAMINATION OF THE TRANSITION

In this section, we describe the data we collect on the U.S. broadcast television market and test the predictions of the economic models.

### A. Data

To analyze stations' decisions and test the implications of our models, we gathered data from a variety of sources.<sup>155</sup>

#### 1. Stations' Decisions and Characteristics

The stations' transition decisions are taken from FCC reports stating which stations switched to DTV before February 17, which switched on that date, and which planned to switch then but changed

---

154. Nash equilibrium depends on the relative sizes of  $\Delta_1$ ,  $\Delta_2$ ,  $d_1$ , and  $d_2$ . The various permutations of the magnitudes boil down to four cases for Nash equilibrium in pure strategies; see JAMES MILLER & JAMES E. PRIEGER, *THE BROADCASTERS' TRANSITION DATE ROULETTE: STRATEGIC ASPECTS OF THE DTV TRANSITION 24-25* (Aug. 20, 2009). The economic fundamentals in the market (viewership, costs, and the expected loss of viewership upon transition) determine into which case the market falls.

155. No confidential FCC data are used, although some data come from proprietary industry databases as noted below.

their decision in response to FCC action.<sup>156</sup>

The local viewing market, the state of location, network affiliation of a station, and viewership is from Warren's *TV and Cable Factbook* proprietary database.<sup>157</sup> Only full-power stations are included in our data. Viewership is measured as the number of noncable viewing households who watched the station at least once in the week, averaged over the weeks of Nielsen's sweeps month. Viewing households outside the home DMA of the station, if any exist, are included in the count. Since the count of noncable households includes subscribers to alternative distribution systems such as satellite, we adjust viewership by multiplying the figure by the fraction in the DMA of noncable viewers that receive programming over the air (OTA).<sup>158</sup> Our resulting measure is an estimate of  $q_i$ , the OTA viewership stations had before the February 2009 decision period. In the estimations we multiply the latter viewership variable by the ad price per viewer (described in the next section), to measure  $pq^0$ , the revenue importance of the viewership at stake.

We also gathered data pertaining to  $\Delta_i$ , the change in the cost of the electricity input. We make one change from the theoretical model: since most stations were already broadcasting in DTV by February 2009, the change in the energy bill for a station comes from turning off the analog transmission. The change in the power requirement from completing the switch to DTV (measured as the input power required for the analog transmission) is estimated from public FCC sources.<sup>159</sup>

156. See generally FCC Releases Lists of Stations Whose Analog Operations Terminate Before February 17, 2009, or that Intend to Terminate Analog Operations on February 17, 2009, *Public Notice*, 24 FCC Rcd. 1416 app. A (2009) (Feb. 10, 2009) (for stations terminating analog broadcasting before February 17 and for stations planning to terminate on February 17); see generally FCC Releases Lists of TV Stations Responses to Requirements for Analog Termination on February 17, 2009, *supra* note 145, app. A-C (for which stations were allowed to actually terminate on February 17). See also *supra* Part III.B.

157. All variables except viewership are from the online subscription database and are current as of the decision time (February 2009). Viewership is from the 2008 printed copy of the Factbook; see generally WARREN COMM'N NEWS, TELEVISION AND CABLE FACTBOOK 2008 (2007).

158. The latter variables are from the Television Bureau of Advertising website, TVB.org, and are for February 2009. <http://www.tvb.org/> (last visited May 13, 2011).

159. The peak power transmitted by a station's digital and analog antenna can be found from the FCC's Media Bureau Consolidated Database System ("CDBS"); see *Index of Media Bureau CDBS Public Database Files*, FED. COMM'N COMM'N. <http://www.fcc.gov/mb/databases/cdbs/> (last visited Jan. 27, 2011). For analog stations, this includes only the visual power transmitted. However, total peak power also includes aural power. Furthermore, to find the prime (input) power requirement for broadcasting, one must also consider the relationship between average and peak power and the "cabinet efficiency" in converting input power to RF. Based on discussions with staff from the FCC's Office of Engineering and Technology, we assumed that the aural/visual power ratio was 0.2 for VHF

The data needed to estimate the power requirement for analog broadcasting is available for only about 74 percent of commercial stations, which reduces the sample size of estimations including this variable. The price of electricity facing each station is taken to be the state average commercial retail electricity price for the first quarter of 2009, from the Energy Information Administration.<sup>160</sup> The product of the latter two variables is our estimate of the cost savings per hour of broadcasting from turning off analog transmission.

Two variables relate to  $\phi_i$ , which is the expected fraction of viewers lost because of the transition. The FCC released estimates of the interference a station's digital broadcast was expected to receive from other broadcasts in the area, and we use the fraction of the DTV broadcast footprint so affected.<sup>161</sup> The second variable is an estimate of the loss in population covered by the broadcast of the station when switching to digital transmission is publicly available from the FCC for some stations, and it is known to be less than 2 percent for the rest.<sup>162</sup>

## 2. Market Information

We take the relevant market for a station to be the Nielsen DMA in which the station is licensed.<sup>163</sup> While a station's footprint does not exactly match a DMA, and not all stations overlap fully with each other within a DMA, the DMA is the standard market definition for television broadcasting in industry and in academic research.<sup>164</sup>

stations and 0.1 for UHF stations, that the cabinet efficiency was 0.7 for analog transmission and 0.5 for DTV, and that average visual power is 0.37 times peak visual power for analog transmission (the latter consideration is irrelevant for DTV). Starting with the "peak power transmitted" found in the CBDS,  $x$ , the assumptions imply that our estimate of prime power,  $y$ , is  $y = (0.37 \times x + 0.2 \times x)/0.7$  for NTSC (analog) VHF stations,  $y = (0.37 \times x + 0.1 \times x)/0.7$  for NTSC (analog) UHF stations, and  $y = x/0.5$  for DTV stations.

160. See ENERGY INFO. ADMIN., ELECTRIC POWER MONTHLY, June 2009, at 108, tbl.5.6B.

161. See Advanced Television Systems and Their Impact on the Existing Television Broadcast Service, *Memorandum Opinion and Order on Recon of the Seventh R&O and Eighth R&O*, 23 FCC Rcd. 4220 app. B (2008).

162. *Archive of Map Book for Full-Service Digital Television Stations Having Significant Changes in Coverage*, FEDERAL COMM'N COMM'N, available at <http://www.fcc.gov/dtv/markets/report2.html> (last visited Jan. 27, 2011). The data on population covered is available for the 319 stations for which FCC analysis showed that more than two percent of the population covered by the station's analog service would not be covered by its digital service.

163. The Designated Market Area is a geographic area defined by Nielsen Media Research Company. Each DMA is a group of counties comprising the major viewing audience for the television stations located in the metropolitan area. DMAs are substantially similar to the Standard Metropolitan Statistical Areas ("SMSAs") defined by the Census Bureau. There are 210 DMAs in our analysis.

164. See generally Keith Brown & Peter J. Alexander, *Market Structure, Viewer Welfare, and*

DMA level variables were collected from the *SRDS Media Solutions* database, which includes demographic variables from Claritas and ad price data from SQAD.<sup>165</sup> We supplemented this primary source with data from Nielsen on the number of TV households in each DMA,<sup>166</sup> from TVB on the number of OTA-only households,<sup>167</sup> and from the NTIA on the waitlists for DTV converter box coupons at the time of the transition.<sup>168</sup> We also collected data from a Nielsen report on the state of DTV “readiness” just before the transition, which are available only for a small subset of DMAs.<sup>169</sup> Two variables are available: the fraction of households that are completely unready and those partially unready for the digital transition.<sup>170</sup> For use in DMA-level analysis, we calculated a weighted average electricity price (see above for source) based on the number of stations located in each state when a DMA spans states.

### B. Empirical Results

We conducted our analysis at two levels: market and individual station. Summary statistics for the data are in Tables 1 and 2.

#### 1. Market Level Analysis

We begin with a summary of the market-level transition decisions. We calculate the fraction of stations within each DMA that transitioned before, on, and after February 17, and present summary statistics for the 210 observations (one per DMA) of these variables in Table 3. On average in a DMA, 25 percent of stations switched on February 17.

*Advertising Rates in Local Broadcast Television Markets*, 86 ECON. LETTERS 331, 331–337 (2005).

165. The ad prices are the SQAD Cost-Per-Point (“CPP”) in the DMA the previous quarter (4Q08). The ad prices per viewer that we use are derived from the CPP as follows. Let  $p$  = ad price per viewers,  $s$  = SQAD CPP,  $r$  = Nielsen rating points,  $V$  = viewing TV households,  $T$  = TV households, and  $A$  = ad price. The CPPs, when multiplied by the relevant Nielsen rating points, yield the average ad cost in the DMA, and so  $A = sr$ . Since one ratings point represents one percent of the total number of TV households, we have  $r = 100V/T$ . Since  $p = A/V$ , we have:  $p = sr/V = 100s/T$ . We observe both  $s$  and  $T$  in the data, and use them to thus calculate  $p$ .

166. See *Local Television Market Universe Estimates: Comparisons of 2008–09 and 2009–10 Market Ranks*, NIELSEN (last visited Jan. 27, 2011).

167. Data are for February, 2009, taken from the Television Bureau of Advertising website. See *Local Cable Reach Guide Feb '09*, TVB (last visited Aug. 21, 2009).

168. The NTIA data are from their website. See *Coupon and Household Wait List By DMA*, NTIA 5–15 (Feb. 16, 2009).

169. See *5.7% of U.S. Households – or 6.5 Million Homes – Still Unprepared for the Switch to Digital Television*, NIELSEN (Jan. 22, 2009).

170. Partially unready households have at least one television in the household able to receive DTV programming and one television that cannot. For a completely unready household, no television sets can receive DTV programming.

However, 28 percent of stations on average desired to switch on February 17, so about 3 percent wanted to switch but changed their plans in response to the FCC's imposition of additional requirements. On average, 13 percent of stations had already switched before February 17, giving a total of 38 percent on average that switched on or before February 17. This means that about two of the eight stations in an average DMA switched on February 17, one station switched before that, and the remaining five waited until later to turn off analog broadcasting. There are some markets where no station switched, and other markets where all switched early. In both cases, particularly the latter, these are usually markets with few (or even only a single) stations.

For each statistic, the median is lower than the mean, implying that the distribution is not symmetric. For example, in the median DMA, one of five stations switched on February 17 and only 33 percent transitioned early. The full distribution is shown in Figure 1. This histogram shows that in 31 markets, no station transitioned early, and in 13 markets, all did. In the middle range, the weight of the distribution is toward the low end (representing not switching early).

To characterize how the decisions relate to market characteristics, we calculate correlation coefficients between the fraction of stations switching early (on or before February 17) and a host of demographic and economic variables. The results are in graphical form in Figure 2, with the correlation coefficient on the  $y$ -axis. Although we will mention which results are in accord with the theoretical models, the presentation is for descriptive purposes only. Some of the correlations may suggest, but none implies, causality because the pairwise correlation coefficients do not control for other factors.

Panel (a) of Figure 2 shows that switching early is negatively correlated with the size of the market, whether size is measured by the number of stations, the number of households with televisions, households receiving OTA-only broadcasts (i.e., no subscription television), total households, or the adult population in the DMA. All but the first correlation are significant.<sup>171</sup> These measures of market size are proxies for  $q^0$  in  $d$  from the theoretical model, so finding that larger markets show less early transitioning is in accord with empirical implications 2 and 3 from the models. Note that with market-level data we cannot distinguish between the decision theoretic and game theoretic models.

In panel (b), we show that early switching displays a U-shaped correlation with age of the household head. For the youngest and oldest

---

171. Bars in the darker color on the graphs indicate the statistical significance of the correlation coefficient at the 5 percent level.

age categories, correlation is positive, while it is negative for the middle ages. While this may merely be an artifact of the data, the relationship is remarkably smooth. Given that one recent marketing survey<sup>172</sup> listed the Baby Boomer generation as the most sought-after advertising demographic, and Generation X as the next most sought after, perhaps the significant negative correlations for these groups reflect broadcasters' fears of losing these high-value viewers. This is the interpretation suggested by implications 2 and 3, since presumably ad price  $p$  is highest in areas with large proportions of viewers in these desirable demographic groups. Similarly, panel (c) shows that the highest income brackets also display negative correlation with early transitioning. High-income groups are also valuable viewers in terms of ad sales.

In panel (d), we look at the correlations with racial and ethnic composition. The only significant correlation is with the fraction of population that is Hispanic, which is negative. After Boomers and Gen X'ers, Hispanics are the third most sought-after demographic group for advertisers,<sup>173</sup> and were more than twice as likely as whites to be unready for the DTV transition.<sup>174</sup> Therefore, this finding is also in accord with implications 2 and 3.

We next look in panel (e) at several variables associated with  $\phi$ , the expected fraction of viewers lost from transition. Transitioning early is negatively (but not significantly) correlated with the number of coupon requests, households, and OTA-only households on the NTIA waitlist at the time of the transition (all taken as a fraction of the number of TV households in the DMA). Since these are measures of lack of readiness for the DTV transition, they serve as proxies for  $\phi$ . Thus, implications 2 and 3 predict the negative correlation we find. Early switching is also negatively correlated with Nielsen's two measures of "unreadiness" for transition, the percentage of partially and completely DTV-unready households. Only the latter is significant, but these provide further evidence in accord with the models.

Finally, we look at correlation with ad prices in panel (f). Implication 2 predicts that higher ad prices will be associated with less early transitioning. Although that is the case, no correlations are significant.<sup>175</sup> Not depicted in Figure 2 is the correlation with electricity

172. See Press Release, Anderson Analytics, Marketing Executives Networking Group (MENG) Releases First Annual Survey of Top Marketing Trends for 2008 (Nov. 27, 2007), available at <http://www.andersonanalytics.com/newsfiles/20071127.pdf>.

173. *Id.*

174. As of February 1, 2009, 8.5 percent of Hispanic TV households were unready for the transition, compared to 4.1 percent of white households. See *3.1% of U.S. Homes Still Unready for Digital Transition*, NIELSEN (May 1, 2009).

175. The ad prices are split by daypart, which are Prime Access (6 - 7 PM), Prime (7 - 10

prices, which is positive, in accord with implication 1 but is small and insignificant. The unemployment rate in the DMA is not significantly correlated with the transition decision, although to the extent that local economic conditions affect local ad prices, the model suggests it might be.

In summary, the analysis of the DMA-level data shows that stations were less likely to switch to DTV-only broadcasting in markets where the cost of losing viewers was higher and where households were less ready for the transition. However, such results, while consonant with the implications of the economics models of the stations' decision-making, require further exploration. Given the correlation among many of the market and demographic variables, multiple regression techniques are required to make a stronger case for the causal impact of any of these variables on stations' decisions. Furthermore, to distinguish between the decision theoretic model and the game, analysis must be conducted at the level of the station.

## 2. Individual Stations' Decisions

We turn now to our data on the decisions made by individual stations. There are 1,740 stations we analyze, which are the full-power commercial and non-commercial stations broadcasting at the time of the transition in the 50 U.S. states and Washington, D.C.<sup>176</sup> We begin with preliminary analysis of the stations' decisions, and then consider a regression framework to better identify which potentially causal factors matter.

### *a. Preliminary Analysis*

Table 2 and Figure 3 show that 36 percent of the full-power stations transitioned early, switching on or before February 17.<sup>177</sup> Figure 3 reveals considerable variation among networks, however. The three traditional networks were more conservative than most others, switching early only 30-33 percent of the time. FOX and the CW were about average, while Ion and Univision were far below average (16 percent and 17 percent, resp.). PBS and stations in the "other" category (independents, non-PBS public or educational stations, and niche networks) were more likely to switch early than average (44 percent and

PM), Late News (10 - 10:30 PM) and Late Fringe (10:30 PM - 12 AM).

176. We do not include the stations from Puerto Rico, Guam, and the U.S. Virgin Islands in our data, although they appear in the FCC data.

177. The figure differs slightly from the figure in Table 3 of 38 percent because the former is a simple average of stations, and the latter is an average over DMA's of the fraction within the DMA (an [unweighted] average of an average).

40 percent, resp.). PBS does not rely on paid advertising to generate station revenue, and its viewers may be less likely to turn to other networks should problems arise due to the unique nature of public programming. Thus, in terms of the models, the expected revenue cost of transitioning is probably lower for a PBS station, which may explain why so many of them wished to switch early. Finally, the network O&O stations were very unlikely to switch early: only 10 percent did so. The networks ABC, CBS, Fox, and NBC/Telemundo all agreed to delay their DTV transition to June for the stations they owned.<sup>178</sup>

In Figure 4, we break out the transition decision by the quartile of the size of the television market (based on Nielsen rankings of TV markets). As expected, larger markets are associated with a lower probability of switching early.

### *b. Regression Analysis*

In the last part of this section, we present the results from several regressions of the decision to switch early on the station and market characteristics. The regression models allow us to hold constant other factors, allowing cleaner tests of the theory and stronger evidence for (although not proof of) causality.

All estimations are probit regression models with a binary dependent variable.<sup>179</sup> The dependent variable  $y$  takes the value 1 if the station transitioned early (or wanted to, depending on the estimation, as described below), and is 0 otherwise. In a probit model with a vector of regressors  $x$ , the probability that  $y = 1$  is  $\Phi(x\beta)$ , where  $\Phi$  is the cumulative distribution function of the standard normal distribution and  $\beta$  are the regression coefficients. The *marginal effect* of a regressor is the effect of a one unit change in  $x$  on the probability that  $y = 1$  (i.e., on the probability that a station switches early). In Tables 4 and 5, we present the marginal effects (and their standard errors) rather than the (less informative) regression coefficients.<sup>180</sup>

178. See *Network Owned Stations*, HOMETOWN STATIONS TECH. BLOG PAGE (Feb. 9, 2009, 07:36), <http://www.wlio.net/index.php?m=02&cy=09&entry=entry090217-073628> (citing NAB Smart Brief of Feb. 6, 2009). Most of the O&O's that switched were owned by ION and TBN.

179. The regressions are estimated using Stata 11, with the "probit" and "margins" commands.

180. In the familiar ordinary least squares model, the marginal effects are simply the regression coefficients. In nonlinear models such as probit, the two differ. We compute the marginal effects in the tables as the average marginal effects in the sample, using discrete changes in  $x$  for binary regressors and derivatives for continuous regressors. See WILLIAM H. GREENE, *ECONOMETRIC ANALYSIS* § 19.3 (4th ed. 2000).

## 1. Analysis of All Stations' Decisions

In the first two estimations, in Table 4, the dependent variable is 1 if the station actually transitioned early, regardless of what its earlier plans were. Estimation 1 includes all stations, including noncommercial stations and those, which had already transitioned before February 17. Given that the latter are not strategic players in the game modeled above, the results from Estimation 1 are meant to be descriptive only.

In Estimation 1 in Table 4, the size of the market at risk, as measured by the number of OTA-only TV households in the DMA, network indicators, and demographic variables are included. We use OTA-only households to proxy  $q$  in the model instead of total television households (which includes cable and satellite viewers) because OTA viewers are the ones at risk of switching to another station if problems with the transition develop. In Estimation 1, we do not use the station-specific viewership variable, because it is not available for noncommercial stations. A second variable captures the fraction of television households in the DMA that are OTA-only. Although the models above suggest that only the number of OTA viewers matter, not the proportion of viewers that are OTA-only, we include it to account for possible risk aversion on the part of the station (the phenomenon of shying away when "too many eggs are in one basket"). If this form of risk aversion is present on the part of the stations, then even after controlling for the level of OTA-only viewership the fraction of OTA viewers will have an additional negative impact on the likelihood of switching early.

We also control for the number of stations in the market. Given that we do not vary the number of stations in the theoretical models, we add this variable to the econometric models to control for heterogeneity among markets and have no expectation concerning its sign. The demographic controls included are related to the racial composition, ethnicity, age, and income in the DMA.

In accord with our models and the results discussed above (see discussion of Figure 2(a)), market size (as measured by the number of OTA-only households in the DMA) has a large, significantly negative impact on the decision to switch early. The marginal effect of -0.67 for the OTA households variable, which is denominated in millions, implies that an extra million OTA households in the DMA is associated with a 67 percentage point decrease in the probability that the station switches early. The fraction of OTA-only viewers in the DMA has a negative impact, in line with the notion of risk aversion, but it is not statistically significant. We do not include this variable in the following estimations.

The coefficients for the network variables are in accord with the

results in Figure 4. The largest impact among the network variables is for network O&Os. Other things equal, if a station is an O&O it is 26 percentage points less likely to switch early. Consistent with the correlations we found in the DMA-level analysis and the implications of the model, we find significant negative coefficients for Hispanics, the prime age group, and high-income households. Since these variables are proportions, the marginal effects are the increase (in percentage points) of a one percentage point increase in the regressor. For example, the marginal effect of  $-0.40$  for Hispanics implies that an extra percentage point of the DMA population that is Hispanic lowers the probability that a station in the DMA switches early by 0.4 percentage points, *ceteris paribus*. The coefficient for the Asian group is positive, possibly indicating that advertisers perceive them to be a less-desirable demographic segment,<sup>181</sup> but more likely due to the outlying observations from Hawaii.<sup>182</sup>

## 2. Analysis of Commercial Stations' Decisions: Actual Transitions

In Estimations 2 through 4, we limit the sample to commercial stations. The models above tacitly assumed that stations are run commercially for profit, and the profit calculus for noncommercial stations (chiefly PBS stations) may differ. For example, one would not expect ad prices to matter for PBS and educational stations, and including noncommercial stations in the sample would partially obscure the impact of regressors involving ad prices. In the following estimations, we replace the DMA-level market size with the station-specific variable for the OTA viewership (which is available only for commercial stations), multiplied by the advertising price per viewer for a local prime time ad. The latter variable, denoted "OTA viewership revenue/ad" in Tables 3 and 4, is the revenue per ad (in \$1000s) at risk from the transition. Empirical implication 2 from the models suggests that higher ad revenue at risk (due to either higher ad prices per viewer or more viewers) should decrease the likelihood of switching early. We also replace the count of stations with the number of commercial stations in Estimations 2 through 4.

---

181. The marketing report cited above did not rank Asians among the highly sought after demographic groups; see *Press Release, supra* note 172. Asian Americans have also been called the "invisible" demographic on-screen in broadcasting; see Michael Hong, *The Invisible Asian-Americans*, 135 BROAD. & CABLE 78 (2005).

182. All Hawaiian stations switched early, and the Honolulu DMA has a fraction of Asians that is twice as high as the next highest DMA. If Hawaii is dropped from the sample, then the Asian marginal effect loses statistical significance.

In Estimation 2, also in Table 4, the marginal effect of *OTA viewership revenue/ad* is negative and highly statistically significant, as suggested by the theory. The marginal effect of -0.21 means that when the ad revenue per ad from OTA viewers for the station rises by one thousand dollars per ad, the likelihood the station switches early falls by about a fifth of a percentage point.<sup>183</sup> Thus, when the opportunity cost of switching from the financial impact of potentially lost viewers rises, stations are significantly less likely to switch early.

Also new to Estimations 2 through 4 is a variable pertaining to the stations' benefits from switching. We include the power savings from turning off analog transmission multiplied by the electricity price, denoted *Electricity Price*  $\times$  *Power* in Tables 4 and 5. Due to the skewed nature of the power cost savings, it enters the regression in log form. In Estimation 2, we find a positive and statistically significant coefficient for the power cost variable, as expected from empirical implication 1 from the models. The marginal effect of 0.042 for the log of *Electricity Price*  $\times$  *Power* implies that when the regressor doubles (a 100 percent increase) it increases the probability of switching early by 4.2 percentage points. Thus, when the benefit to switching from reduced operating costs rises, stations are more likely to switch.

### 3. Analysis of Commercial Stations' Decisions: Desired Transitions

Since we want to focus on the strategic aspects of the decision as modeled above, rather than outcomes influenced by regulatory decree apart from direct profit considerations, we further refine our dependent variable and sample for Estimations 3 and 4 (Table 5). The dependent variable in these estimations is the decision made to transition early, before the FCC intervened in the final week and some stations backed away from their plans they had announced earlier. Any station that transitioned before February 17 is removed from the sample, since its decision was already made and it neither faced the decision problem nor played the strategic game modeled above. There are still over 800 stations in the sample for Estimation 3.

The impacts of the variables included in Estimation 2 pertaining to the stations' benefits and costs from switching are similar in Estimation 3. That is, the significance and magnitude of the marginal effects of *OTA viewership revenue/ad* and *Electricity Price*  $\times$  *Power* are about the same in Estimations 2 and 3. The new variables in Estimation 3 pertain to the

---

183. An increase in *OTA viewership revenue/ad* of \$1,000 corresponds to an increase of one-third of a standard deviation of this variable.

expected fraction of viewers lost through the transition ( $\phi_i$  in the theory models). As such, we expect their coefficients to be negative. The first is the expected interference with a station's DTV broadcast from the other stations in the DMA. The impact of the interference is negative as expected, but insignificant in Estimations 3 and 4.

The other variable related to  $\phi_i$  is the fraction of potential analog viewers that would not be able to receive a digital broadcast (*% Pop. lost by transition*). Since the variable is not observed in the public FCC data when it is under two percent of the population, in the regression specification we let those stations be the omitted category and allow the other stations' variable to enter as a two-part linear spline.<sup>184</sup> The spline was found to be necessary to remove the undue influence of a few outliers (the top 2 percent of observations). The main part of the spline, for stations potentially losing between two and 32 percent of their analog viewers, has a statistically significant and negative marginal effect. The magnitude of the effect implies that when the population losing the station's broadcast increases by one percentage point in this region, the station's likelihood of switching decreases by 0.81 percentage points, *ceteris paribus*. The marginal effect for the top part of the spline is positive but not even close to being statistically significant. Thus, in accord with the models, the variables capturing the danger of losing viewers during the transition are generally associated with a lower likelihood of switching.

The first three estimations explore variables pertaining to the first two empirical implications, which apply equally to the decision theoretic and game theoretic models. To explore specifically whether stations are acting strategically, we test implication 3 from the game theoretic model by including in Estimation 4 three variables that pertain to  $d_j$ , a station's rival's revenue cost of switching early. Recall that when the rival switches early and puts its viewers at risk, the rival's loss becomes the station's gain. Implication 3 suggests that when the rival switches early, a variable pertaining to  $d_j$  should have the same impact on a station's decision as if it pertained to  $d_i$ —that is, was a station's own characteristic. We include variables measuring the average of the OTA viewership revenue per ad, the DTV interference, and the population lost by switching for the *other* stations in the DMA. Since implication 3 applies only when the rival switches early (because that is the only way a station might gain its viewers), when calculating the averages we include only other stations that wished to switch early.<sup>185</sup> The game implies that each of these

184. For a discussion of splines in regression, see GREENE, *supra* note 180, § 8.2.6.

185. A possible objection to only including other stations that wanted to switch early is that a station would not observe which those would be until after its own decision had to be

variables should have negative marginal effects.

If the stations are not acting strategically, and pay no attention to their rivals' expected actions, then characteristics of the other stations in the DMA should have no impact on a station's decision. However, for a clean test of this hypothesis, we need to correct for potential endogeneity of the other stations' characteristics. Since only stations switching early are included in the average of other stations' characteristics, if there are unobserved causal factors in the DMA that affect all stations' incentives to transition, then the new variables in Estimation 4 will be endogenous in the regression. Such endogeneity would invalidate the results of probit estimation, by finding a link between rival's characteristics and the decision of a station to switch that is driven by the unobserved common factor in the DMA rather than the strategic interactions we wish to isolate. Our solution is to add DMA-level fixed effects to the estimation, removing the influence of unobserved factors in the DMA.<sup>186</sup> A consequence of using a fixed-effects estimation is that any variable not varying within the DMA (such as the demographic variables) is absorbed into the fixed effects, and any observations from any DMA with no variation in the dependent variable are dropped. This reduces the sample size to 504 stations in Estimation 4.

The results in Estimation 4, also in Table 5, are in line with the game theory, suggesting that stations are indeed acting strategically. The more ad revenue from OTA viewers the rival stations transitioning on February 17 have, the less likely a station is to switch itself. The impact is large (twice as large as the marginal effect of the station's own ad revenue variable) and statistically significant at the 1 percent level. Furthermore, the more population lost by rival stations, the lower the probability that a station transitions early. The marginal effect is again larger than the own-station variable's impact and is highly significant. The impact of the interference the rival stations are likely to have is negative, in accord with

---

made. However, in the Nash equilibrium of a full information game such as ours, each player chooses its best action in response to what it expects the other players to do, and its expectations turn out to be correct.

186. See BADI H. BALTAGI, *ECONOMETRIC ANALYSIS OF PANEL DATA* § 2.2 (3d ed. 2005) (for fixed effect models generally); *see id.* § 11.1 (for the probit fixed effect model). In general, fixed effects models remove the endogeneity problems caused by variables that are correlated with unobserved factors common to the unit of observation (the DMA, in our case). There is a technical issue regarding the asymptotic properties of the probit fixed effects model that affects the consistency of the regression coefficients (the "incidental parameters problem"). We use the probit model nevertheless in Estimation 4 for consonance with the previous estimations. When the specification in Estimation 4 is estimated with either the linear probability fixed effects model or the conditional logit model (results not shown), neither of which suffers from the incidental parameters problem, our conclusions regarding the sign and significance of the marginal effects of the strategic variables are unchanged.

the theory, but statistically insignificant. For all three of the “strategic”  $d_j$  variables, which are jointly statistically significant,<sup>187</sup> the marginal effects are larger than impact of the corresponding  $d_i$  variable, highlighting the importance of the strategic considerations. The signs of the other variables in Estimation 4 are similar to those in Estimation 3.<sup>188</sup>

## CONCLUSIONS

Throughout the history of the broadcast industry, regulators have faced difficult decisions in determining how best to fulfill their statutory mandate to serve the public interest when changing technology promises new benefits for consumers but threatens to leave some behind. While we have focused on the DTV transition, issues such as standard setting, coordination of industry and consumers on all sides of a network market, backward compatibility, and the proper balance between economic incentives and regulatory compulsion have arisen in many situations. Some innovations, such as FM radio broadcasting, color television, or the use of the telephone network for Internet access, have succeeded in the marketplace, while others (e.g. AM stereo radio) have failed. Regardless, regulators are better able to design appropriate rules—and to evaluate the success of the regulatory efforts—when they understand the financial and strategic incentives facing industry participants.

The models introduced in this article prove to be useful tools for understanding the strategic thinking of the broadcasting entities. The decision theoretic model formalizes the natural intuition that stations choose to transition earlier when the benefits are higher or the costs are lower. Empirical testing of the model yields results that are in line with the predictions. A more interesting (and less obvious) set of results comes from the game theoretical model, which shows that when a station’s management also considers what its rivals will do, the audience size of the other stations (as well as the chances that the station might gain

---

187. A test of the joint statistical significance of the three variables new to Estimation 4 returns a chi-square(3) statistic of 42.9, with a  $p$ -value of nearly 0.

188. Some readers of early versions of this article noted that since stations faced many times when they could have chosen to switch to DTV before February 17, 2009, that perhaps the econometric model should account for the multiple decision periods. One way to do this is to change the dependent variable to an ordinal variable taking value 0 if switched after February 17, 1 if switched on February 17, and 2 if switched before then. Then an ordered probit model can be used in place of the simple probit. Repeating Estimations 2 and 3 with this new definition of the dependent variable and the ordered probit model yields results that are substantially similar to those presented in Tables 4 and 5. In particular, the coefficients of the viewership, power cost, and ad price variables that are significant in the probit model are also significant (with the same signs) in the ordered probit model. The exception is the % *Pop. lost by transition* variable, the coefficient of which has the same sign as in the probit model but is not significant in the ordered probit model.

some of these viewers) becomes strategically important.

One insight from the game is that when many players (or, equivalently, players with a large share of consumers) are expected to switch to the new technology early, the incentives for other players to delay increases. These strategic incentives make it more difficult than it otherwise would be for all players in a market to coordinate their actions on adopting the new technology. In situations where the regulator wishes the transition to proceed uniformly, it may want to give more preference to mandatory cutoffs than to purely voluntary measures in such cases. In the present case of the DTV transition, however, the strategic incentive for some stations to delay was in accord with the FCC's desire to protect consumers in certain "at risk" markets by ensuring that some analog viewing options remained temporarily after February 2009.

Given that today's technological *dernier cri* may quickly become yesterday's obsolete historical curiosity, it is certain that the DTV transition will not be the final technological sea change that the FCC will oversee, perhaps even in broadcasting. Insights gained from this examination may thus provide useful to future regulatory endeavors.

| Variable                      | Mean      | Std. Dev. | Min   | Max        |
|-------------------------------|-----------|-----------|-------|------------|
| Stations                      | 8.319     | 5.204     | 1.000 | 27.000     |
| TV households                 | 545,032   | 831,576   | 3,940 | 7,433,820  |
| OTA-only households           | 60,207    | 87,275    | 370   | 798,570    |
| Households                    | 551,089   | 825,845   | 4,000 | 7,546,000  |
| Adult pop                     | 1,105,026 | 1,733,035 | 7,600 | 15,900,000 |
| Age0_18                       | 0.002     | 0.001     | 0.000 | 0.005      |
| Age18_24                      | 0.056     | 0.015     | 0.029 | 0.142      |
| Age25_34                      | 0.158     | 0.017     | 0.113 | 0.220      |
| Age35_44                      | 0.182     | 0.018     | 0.100 | 0.236      |
| Age45_54                      | 0.207     | 0.013     | 0.162 | 0.271      |
| Age55_64                      | 0.170     | 0.012     | 0.131 | 0.212      |
| Age65up                       | 0.225     | 0.035     | 0.111 | 0.369      |
| White                         | 0.810     | 0.124     | 0.288 | 0.976      |
| Black                         | 0.097     | 0.107     | 0.000 | 0.592      |
| Asian                         | 0.024     | 0.041     | 0.000 | 0.507      |
| Race_other                    | 0.068     | 0.067     | 0.010 | 0.355      |
| Hispanic                      | 0.096     | 0.145     | 0.004 | 0.940      |
| HH income \$10-20K            | 0.132     | 0.027     | 0.058 | 0.206      |
| HH income \$20-35K            | 0.229     | 0.026     | 0.133 | 0.278      |
| HH income \$35-50K            | 0.196     | 0.015     | 0.152 | 0.229      |
| HH income \$50-75K            | 0.187     | 0.024     | 0.117 | 0.235      |
| HH income \$75-100K           | 0.094     | 0.025     | 0.048 | 0.167      |
| HH income \$100-125K          | 0.030     | 0.013     | 0.010 | 0.083      |
| HH income \$125-150K          | 0.016     | 0.008     | 0.004 | 0.053      |
| HH income above \$150K        | 0.023     | 0.012     | 0.007 | 0.085      |
| Female                        | 0.512     | 0.010     | 0.474 | 0.532      |
| Commercial Electricity Price  | 9.539     | 2.441     | 6.090 | 20.890     |
| Unemployment rate             | 0.064     | 0.024     | 0.029 | 0.274      |
| Ad price/viewer, prime access | 0.025     | 0.023     | 0.008 | 0.305      |
| Ad price/viewer, prime        | 0.046     | 0.049     | 0.016 | 0.635      |
| Ad price/viewer, late news    | 0.032     | 0.032     | 0.012 | 0.431      |
| Ad price/viewer, late fringe  | 0.024     | 0.032     | 0.007 | 0.431      |
| NTIA waitlist: coupons        | 0.036     | 0.011     | 0.008 | 0.080      |
| NTIA waitlist: households     | 0.020     | 0.006     | 0.005 | 0.042      |
| NTIA waitlist: OTA-only HH's  | 0.009     | 0.003     | 0.002 | 0.020      |
| % HH's partially unready      | 12.634    | 3.919     | 4.930 | 22.170     |
| % HH's completely unready     | 5.400     | 2.275     | 1.760 | 12.240     |

Table notes: there are 210 DMAs. All variables are observed for each DMA except the Nielsen unreadiness figures, which are available for 56 markets.

**Table 1: Summary Statistics for the DMA Level Data**

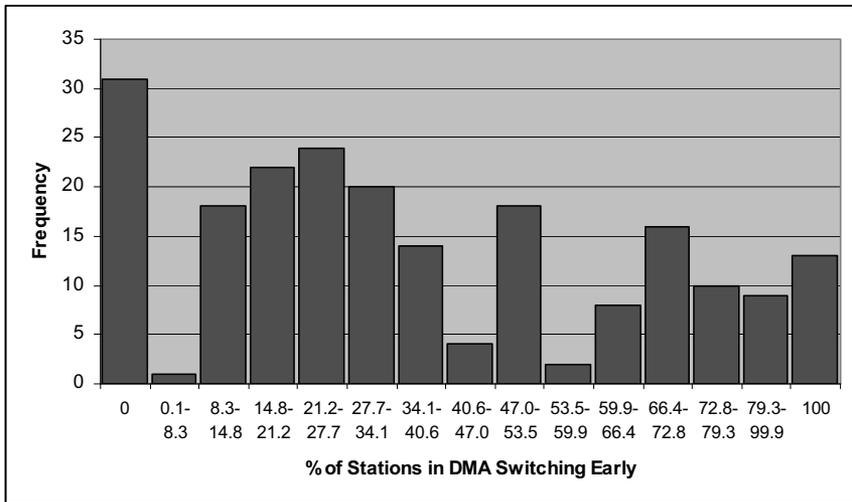
| Variable                                  | Obs   | Mean   | Std. Dev. | Min    | Max    |
|---|-------|--------|-----------|--------|--------|
| Switched on Feb. 17, 2009                 | 1,740 | 0.236  | 0.425     | 0.000  | 1.000  |
| Desired to switch on Feb 17               | 1,740 | 0.261  | 0.439     | 0.000  | 1.000  |
| Switched before Feb. 17                   | 1,740 | 0.124  | 0.329     | 0.000  | 1.000  |
| Switch on or before Feb. 17               | 1,740 | 0.359  | 0.480     | 0.000  | 1.000  |
| OTA-only households in DMA (M)            | 1,740 | 0.096  | 0.125     | 0.000  | 0.799  |
| OTA viewership of station (M)             | 1,245 | 0.029  | 0.051     | 0.000  | 0.498  |
| OTA viewership revenue/ad (\$K)           | 1,245 | 1.175  | 2.968     | 0.000  | 37.455 |
| Stations in DMA                           | 1,740 | 11.549 | 6.176     | 1.000  | 27.000 |
| Commercial stations in DMA                | 1,374 | 9.217  | 5.155     | 1.000  | 25.000 |
| Network: ABC                              | 1,740 | 0.122  | 0.327     | 0.000  | 1.000  |
| Network: CBS                              | 1,740 | 0.126  | 0.332     | 0.000  | 1.000  |
| Network: NBC                              | 1,740 | 0.128  | 0.334     | 0.000  | 1.000  |
| Network: FOX                              | 1,740 | 0.111  | 0.314     | 0.000  | 1.000  |
| Network: CW                               | 1,740 | 0.057  | 0.232     | 0.000  | 1.000  |
| Network: ION                              | 1,740 | 0.035  | 0.184     | 0.000  | 1.000  |
| Network: PBS                              | 1,740 | 0.203  | 0.402     | 0.000  | 1.000  |
| Network: Univision                        | 1,740 | 0.024  | 0.152     | 0.000  | 1.000  |
| Hispanic                                  | 1,740 | 0.108  | 0.141     | 0.004  | 0.940  |
| Asian                                     | 1,740 | 0.036  | 0.068     | 0.000  | 0.507  |
| Black                                     | 1,740 | 0.098  | 0.100     | 0.000  | 0.592  |
| Other race                                | 1,740 | 0.078  | 0.070     | 0.010  | 0.355  |
| Age 25-54                                 | 1,740 | 0.554  | 0.035     | 0.434  | 0.637  |
| Household Income > \$100,000              | 1,740 | 0.079  | 0.039     | 0.022  | 0.219  |
| Commercial Electricity Price (cents/KWH)  | 1,740 | 9.688  | 2.784     | 6.090  | 20.890 |
| Ad price/viewer, prime (\$)               | 1,740 | 0.037  | 0.023     | 0.016  | 0.635  |
| NTIA waitlist (households)                | 1,740 | 0.020  | 0.005     | 0.005  | 0.042  |
| Estimated input power (analog, KW)        | 1,300 | 40.270 | 65.684    | 0.000  | 1342.9 |
| Electricity price × power (log)           | 1,299 | -1.447 | 1.162     | -7.732 | 2.988  |
| Power savings, digital vs. analog (KW)    | 1,030 | 5.600  | 4.671     | -134.9 | 1310.3 |
| % DTV interference (pop.)                 | 1,738 | 0.017  | 0.045     | 0.000  | 0.565  |
| % pop. lost by transition is observed     | 1,740 | 0.163  | 0.370     | 0.000  | 1.000  |
| % pop. lost by transition (when observed) | 284   | 0.108  | 0.113     | 0.020  | 0.714  |

Table notes: the variable “% pop. lost by transition” is observed in the FCC public data only for stations for which it is greater than 2%.

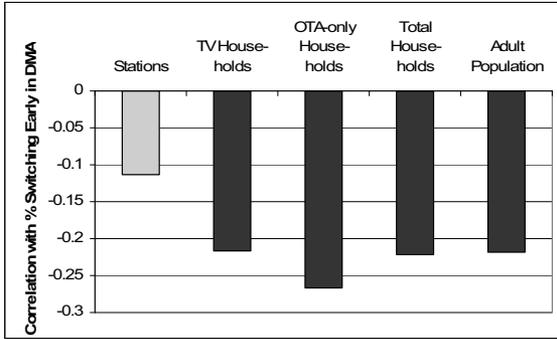
**Table 2: Summary Statistics for the Station Level Data**

| Variable                          | Mean  | Median | Std. Dev. | Min | Max |
|-----------------------------------|-------|--------|-----------|-----|-----|
| Fraction of stations in DMA that: |       |        |           |     |     |
| Switched on Feb. 17               | 0.247 | 0.2    | 0.235     | 0   | 1   |
| Desired to switch on Feb 17       | 0.283 | 0.222  | 0.258     | 0   | 1   |
| Switched before Feb. 17           | 0.133 | 0      | 0.207     | 0   | 1   |
| Switch on or before Feb. 17       | 0.380 | 0.333  | 0.292     | 0   | 1   |

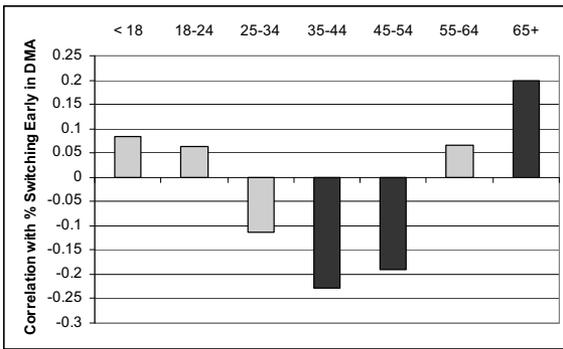
**Table 3: Summary Statistics for Stations' Decisions to Turn off Analog Broadcasting**



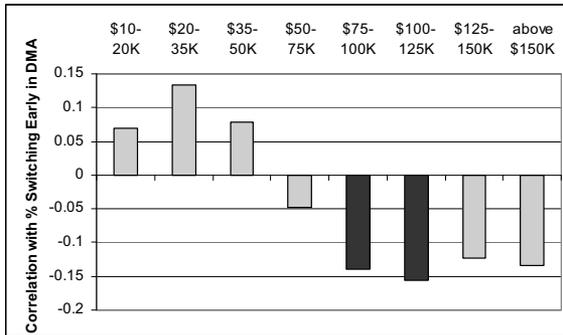
**Figure 1: Histogram of Stations' Decisions to Switch Early**



(a) Correlation with Size of Market

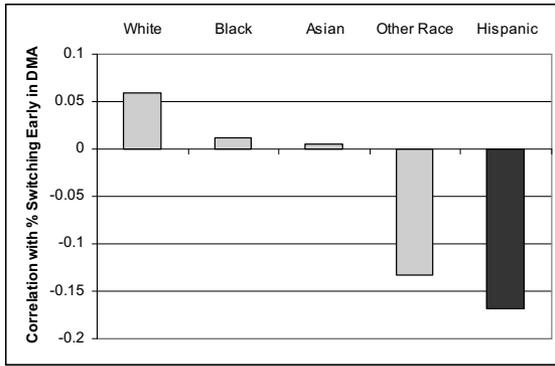


(b) Correlation with Age of Head of Household

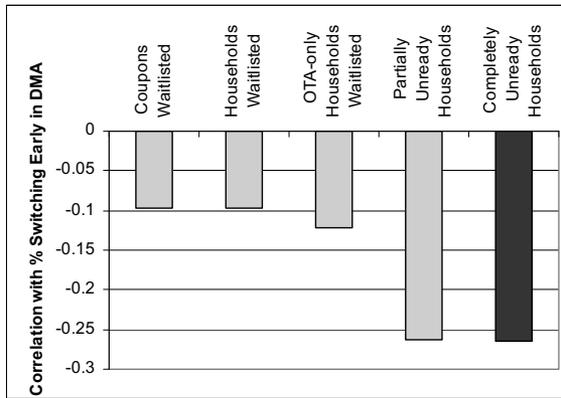


(c) Correlation with Household Income

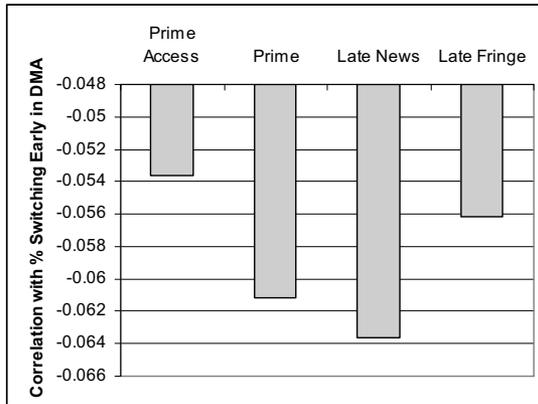
Figure 2: Correlation of Stations' Decisions to Stop Analog Broadcasting Early with Various Factors (DMA level data) – Continued on Page 496



(d) Correlation with Race and Ethnicity



(e) Correlation with NTIA Waitlist for Converter Coupons and Household DTV Readiness



(f) Correlation with Ad Price per Viewer, by Daypart (SQAD Data)  
 Note: lighter bars indicate that the correlation is not statistically significant at the 5% level.

**Figure 2: Correlation of Stations' Decisions to Stop Analog Broadcasting Early with Various Factors (DMA level data) – Continued From Page 495**

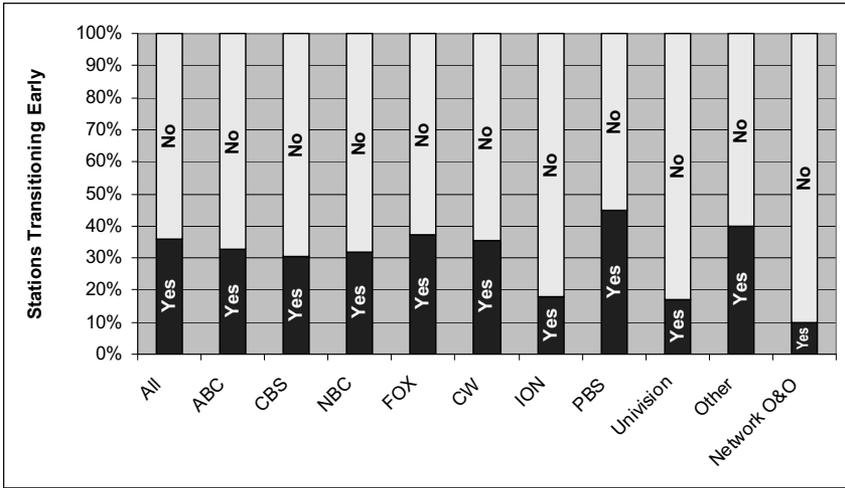


Figure 3: Transition Decisions by Network

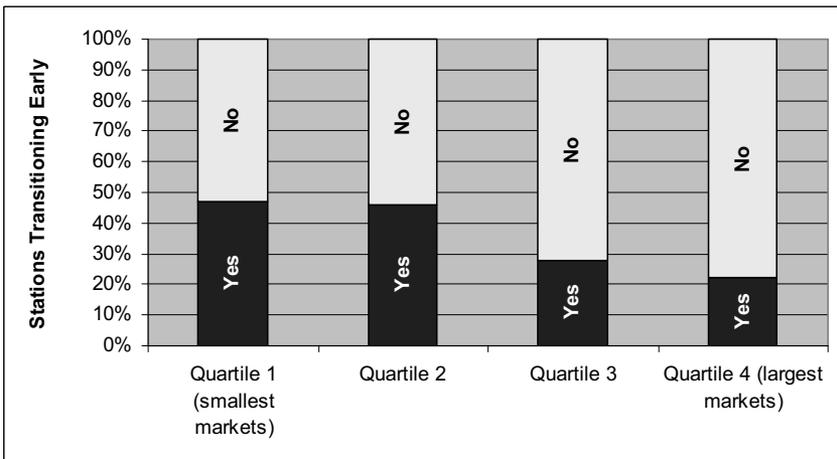


Figure 4: Transition Decisions by Nielsen TV Rank Quartiles

| <i>Y = Actually Transitioned Early</i> | Estimation 1    |         | Estimation 2        |         |
|--|-----------------|---------|---------------------|---------|
|  | All Stations    |         | Commercial Stations |         |
| Variable                               | Marginal effect | s.e.    | Marginal effect     | s.e.    |
| OTA-only households in DMA             | -0.673**        | 0.167   | 0.153               | 0.293   |
| OTA viewership revenue/ad              |                 |         | -0.213**            | 0.031   |
| % OTA-only in DMA                      | -0.448          | 0.306   |                     |         |
| Stations in DMA                        | 0.004           | 0.003   |                     |         |
| Commercial stations in DMA             |                 |         | -0.005              | 0.005   |
| Network owned & operated               | -0.263**        | 0.034   | -0.265**            | 0.037   |
| Network: ABC                           | -0.164**        | 0.033   | -0.041              | 0.048   |
| Network: CBS                           | -0.176**        | 0.032   | -0.038              | 0.051   |
| Network: CW                            | -0.015          | 0.084   | -0.015              | 0.056   |
| Network: FOX                           | -0.115**        | 0.037   | -0.004              | 0.051   |
| Network: ION                           | -0.172**        | 0.033   | -0.107              | 0.090   |
| Network: NBC                           | -0.092*         | 0.046   | -0.085              | 0.048   |
| Network: PBS                           | -0.056          | 0.033   |                     |         |
| Network: Univision                     | -0.128          | 0.075   | -0.131              | 0.079   |
| Hispanic                               | -0.398**        | 0.154   | -0.032              | 0.202   |
| Asian                                  | 1.144**         | 0.322   | 1.136*              | 0.472   |
| Black                                  | -0.078          | 0.127   | -0.468**            | 0.149   |
| Other race                             | 0.533           | 0.317   | -0.352              | 0.413   |
| Age 25-54                              | -1.128*         | 0.463   | -0.759              | 0.541   |
| Income > \$100K                        | -1.187*         | 0.535   | 0.725               | 0.658   |
| Electricity Price × Power (log)        |                 |         | 0.042**             | 0.015   |
| $\chi^2$ stat ( <i>p</i> -value)       | 236.03          | (0.000) | 208.64              | (0.000) |
| Likelihood:                            | -1018.1         |         | -474.4              |         |
| <i>N</i>                               | 1,740           |         | 924                 |         |

\* indicates significance at the 5% level, \*\* indicates significance at the 1% level.

Table notes: Regressions are probit models for the binary dependent variable in the column heading.  $Y = 1$  if station transitioned on or before February 17, 2009, 0 otherwise. In Estimation 2, only commercial stations are included. The marginal effects are the average change in  $\Pr(Y=1)$  in the sample due to a one unit increase in the regressor (approximated with the derivative for continuous regressors). The estimations also include a constant, which does not have a marginal effect.

**Table 4: Probit Regression Analysis of Stations' Decisions to Transition Early to DTV**

| <i>Y = Desired to Transition Early</i>           | Estimation 3        |         | Estimation 4        |         |
|--|---------------------|---------|---------------------|---------|
|  | Commercial Stations |         | Commercial Stations |         |
| Variable   | Marginal effect     | s.e.    | Marginal effect     | s.e.    |
| OTA viewership revenue/ad                        | -0.182**            | 0.028   | -0.332**            | 0.053   |
| Commercial stations in DMA                       | -0.003              | 0.004   |                     |         |
| Network owned & operated                         | -0.248**            | 0.037   |                     |         |
| Electricity price × power (log)                  | 0.049**             | 0.016   | 0.086**             | 0.024   |
| DTV interference                                 | -0.368              | 0.412   | -0.196              | 0.664   |
| % pop. lost by transition<br>(between 2 and 32%) | -0.813*             | 0.359   | -2.177**            | 0.690   |
| % pop. lost by transition<br>(above 32%)         | 1.347               | 1.224   | 5.354               | 5.674   |
| Others' OTA viewership ad<br>rev.                |                     |         | -0.609**            | 0.099   |
| Others' DTV interference                         |                     |         | -1.442              | 1.249   |
| Others' pop. lost by transition                  |                     |         | -5.119**            | 1.701   |
| Network indicator variables                      | included            |         | included            |         |
| Demographic controls                             | included            |         | no                  |         |
| DMA fixed effects                                | no                  |         | included            |         |
| $\chi^2$ stat ( <i>p</i> -value)                 | 178.64              | (0.000) | 258.88              | (0.000) |
| Likelihood:                                      | -407.5              |         | -199.6              |         |
| <i>N</i>   | 831                 |         | 504                 |         |

\* indicates significance at the 5% level, \*\* indicates significance at the 1% level.

Table notes: Sample includes only stations not transitioning before February 17. Regressions are probit models for the binary dependent variable  $Y = 1$  if station planned to transition on February 17, 0 otherwise. The *pop. lost by transition* variable enters the specification in a two-part linear spline with knot placed at about the 98<sup>th</sup> percentile, and the impact of this variable when it is below 2% is absorbed into the constant. Included in the regression specification but not shown in the table are all the network and demographic variables included in Estimation 2. The last three variables ("Others'  $x$ ") are the average value of  $x$  for the other stations in the DMA that transitioned on February 17. Variables in Estimation 3 but not in Estimation 4 do not vary within a DMA and so are included in the fixed effects. See also notes to previous estimation table.

**Table 5: Probit Regression Analysis – Additional Specifications**



# THE UNFINISHED RADIO REVOLUTION: EIGHT PERSPECTIVES ON WIRELESS INTERFERENCE

J. PIERRE DE VRIES\* AND KALEB A. SIEH\*\*

|  |     |
|--|-----|
| PROGRESS TOWARD RATIONAL SPECTRUM RIGHTS: ARE WE GETTING ANYWHERE?<br><i>ELLEN P. GOODMAN</i> .....  | 505 |
| ECONOMIC PRINCIPLES FOR <i>EX ANTE</i> RULES FOR RADIO<br><i>GREGORY ROSSTON &amp; SCOTT WALSTEN</i> .....   | 509 |
| THE NEED FOR WELL-DEFINED YET NON-EXCLUSIVE RADIO OPERATING RIGHTS<br><i>MICHAEL CALABRESE</i> .....   | 512 |
| FORWARD-LOOKING INTERFERENCE REGULATION<br><i>EVEN KWEREL &amp; JOHN WILLIAMS</i> .....  | 516 |
| THE THREE PS: A RESULTING ENERGY APPROACH TO RADIO OPERATING RIGHTS<br><i>J. PIERRE DE VRIES &amp; KALEB A. SIEH</i> .....   | 519 |
| SPECTRUM “PROPERTY RIGHTS” AND THE DOCTRINE OF ADVERSE POSSESSION<br><i>HAROLD FELD</i> .....  | 523 |
| HOW SHOULD RADIO OPERATING RIGHTS BE DEFINED, ASSIGNED, AND ENFORCED IN ORDER TO OBTAIN THE MAXIMUM BENEFIT FROM WIRELESS OPERATIONS?<br><i>BRUCE JACOBS</i> ..... | 526 |
| DEFINING RADIO RIGHTS: THEORY AND PRACTICE<br><i>CHARLA M. RATH</i> .....  | 528 |

Change is in the air: there are likely to be significant new spectrum allocations as a result of the National Broadband Plan, and the march of technology keeps offering new ways to increase the capacity of wireless systems. However, the revolution begun by the end of “command and control” radio licensing and the shift to a more hands-off regime of flexible-use auctioned licenses and unlicensed operation is incomplete. For example, while there is wide agreement on the importance of flexible

---

\* Senior Adjunct Fellow, Silicon Flatirons Center, University of Colorado, Boulder.

\*\* Research Fellow, Silicon Flatirons Center, University of Colorado, Boulder.

use, the debate over the merits of property rights versus open access have left largely untouched the important matter of defining the optimal operating permissions and governance regime for any new allocations.

The following papers were presented at a half-day conference in Washington, D.C. on Friday, November 12, 2010. The conference set out to address the key unanswered question: How should radio operating rights be defined, assigned, and enforced in order to obtain the maximum benefit from wireless operations? The event was organized by Silicon Flatirons, IEEE-USA, and ITIF, and co-sponsored by CTIA, New America Foundation, and FCBA. Reports summarizing the conference and the post-event roundtable discussion are also available.<sup>1</sup>

This event built on a summit on cross-channel interference at Silicon Flatirons in 2009 that analyzed some of the thorny recent radio interference cases.<sup>2</sup> As the summit showed, inter-licensee conflict is greatest across boundaries of different uses, and the increasing diversity of radio uses and users will only serve to amplify this problem.<sup>3</sup> The definition of cross-channel rights and responsibilities has, to date, been ad hoc; this approach is no longer sustainable given the increasing diversity of uses and users, and the need to pack operations ever closer together in order to meet the demand for wireless capacity.

The conference brought together leading economic and legal thinkers to reframe the discussion and grapple with the neglected questions, such as: Not just debating licenses vs. sharing vs. collective use, but designing an optimum rights regime for whichever of these modes is used; not just who should share with whom, but the rules, rights and procedures that would govern and motivate sharing; and not just whether spectrum is being used efficiently today, but what kinds of rights and processes would motivate the most intensive use.

The first paper frames the problem. Here, Goodman looks at the state of play in wireless regulation and concludes that analysts are coming to consensus in many areas.<sup>4</sup> She takes five lessons from recent experience: (1) Things take longer when no one can be held accountable for interference; (2) a failure or inability to deal with the receiver side of

1. Matthew Montgomery, *The Unfinished Radio Revolution: New Approaches to Handling Wireless Interference*, SILICON FLATIRONS CTR., (Nov. 12, 2010), available at <http://www.silicon-flatirons.org/documents/conferences/2010.11.12-862/TheUnfinishedRadioRevolution.pdf>; Kaleb Sieh, *Perspectives on Radio Operating Rights*, SILICON FLATIRONS CTR. (Nov. 12, 2010), available at <http://www.silicon-flatirons.org/documents/conferences/2010.11.12-862/PerspectivesonRadioOperatingRights.pdf>.

2. J. Pierre de Vries, *Radio Regulation Summit: Defining Inter Channel Operating Rules*, SILICON FLATIRONS CTR. (Dec. 2, 2009), available at <http://www.silicon-flatirons.org/documents/misc/OBSummit/Inter-channelSummitReportv1.0.1.pdf>.

3. *Id.*

4. See *infra* pp. 505-08.

the equation produces sub-optimal entitlements; (3) harmful interference should be a yield sign, not a stop sign; (4) confusing efficient spectrum use with distributional issues is recipe for delay; and (5) the consideration of values associated with spectrum use other than efficiency is under-developed.

The next five papers each make proposals for improving rights definitions. Rosston and Wallsten begin by advancing the importance of a regulatory framework that starts with clear rules, such as using resulting emission rather than transmit power, and allows parties to negotiate efficiency-enhancing changes to those rules.<sup>5</sup> They observe that while well-defined rules are important for both licensed and unlicensed bands, the latter may require stricter rules because trades to maximize efficiency could be prohibitively costly given the diffuse and amorphous group of rights holders. Calabrese continues by arguing for an updated radio regulation regime that promotes pervasive connectivity by defining explicit transmit rights and permissible interference on a band-by-service basis, and recording explicit rights and actual operating parameters of licensees in a public database.<sup>6</sup> This, he argues, will lead to access rights that are more definite, more transparent, and more intensive.

Kwerel and Williams then propose that the FCC revisit its general policy of providing incumbents (those licensed first) protection against any interference resulting from subsequent rule changes since its sequential approach to accommodating change coupled with its interference protection policy toward incumbent uses can be detrimental to putting spectrum to its highest value use.<sup>7</sup> They make two recommendations: Future allocations should self-protect against projected, not just current, adjacent band interference; adjacent band interference protection for incumbents should not be static, but be reduced over time.

De Vries and Sieh argue that the overarching goal of spectrum policy should be to maximize concurrent operation, not minimizing harmful interference; delegate management of interference to operators; and define, assign and enforce entitlements in a way that facilitates transactions.<sup>8</sup> To this end, they propose that the regulator articulates operating rights by using probabilistic resulting-energy transmission permissions and reception protections, stipulate the remedies that attach to an entitlement (i.e. injunctions or damages) when it is issued, and separate its roles as rule maker defining entitlements from adjudicator deciding disputes. Wrapping up the proposals, Feld highlights the

---

5. *See infra* pp. 509-11.

6. *See infra* pp. 512-15.

7. *See infra* pp. 516-18.

8. *See infra* pp. 519-22.

problem of violations of radio regulations and how many of these share elements of the adverse possession doctrine in real property law.<sup>9</sup> He recommends that wireless policy makers develop a mechanism similar to adverse possession and deal with exceptional cases by developing a set of guiding principles rather than through ad hoc rule making.

The final two papers delve into the practical considerations. Jacobs recognizes the importance of clarifying radio operating rights, but emphasizes the difficulty of the task.<sup>10</sup> Many complex implementation questions have to be addressed, and the dynamic nature of technology and incommensurable policy values attached to different services further complicates matters. He encourages establishing a protection level for new licensees to minimize transition costs, and encourages the FCC to generalize the principles and criteria it uses to set the protection level and measurement approach in order to foster a more transparent and predictable set of rights for future proceedings.

Rath argues that defining the theoretical framework for radio operating rights must be informed by the experience licensees have gained resolving interference issues in an increasingly complex and market-oriented RF environment.<sup>11</sup> She gives two examples: the success of clear, enforceable and negotiable rights, such as those governing mobile wireless, that allow for private agreements; and the need for additional enforcement assistance to prevent unauthorized operator-to-licensee interference from sources such as signal boosters.

---

9. See *infra* pp. 523-25.

10. See *infra* pp. 526-27.

11. See *infra* pp. 528-30.

## PROGRESS TOWARD RATIONAL SPECTRUM RIGHTS: ARE WE GETTING ANYWHERE?

ELLEN P. GOODMAN<sup>12</sup>

Analysts from legal, economic, and engineering disciplines have supplied plenty of commentary in the past decade on what ails U.S. spectrum management. At this conference, we have offered a number of competing proposals for how to define the rights of spectrum users to emit signals, the responsibilities of spectrum users to reject noise, how spectrum rights and responsibilities should be recorded, and how conflicts over interference ought to be adjudicated.<sup>13</sup> We have also provided differing views on the proper balance between the prevention of conflicting spectrum uses (frequently called *ex ante* protections) and the resolution of conflicting uses after the fact (*ex post* dispute resolution), as well as varying suggestions for public and private institutional roles.<sup>14</sup>

Notwithstanding difference in the details, it seems that analysts are converging on some important consensus conclusions.<sup>15</sup> These include the following:

- We need much more spectrum made available for mobile broadband
- We need a combination of exclusive rights and shared rights to access spectrum, recognizing that sometimes we will want “easements” or low impact access to spectrum that has otherwise been assigned for exclusive use, sometimes we will want commons spectrum for unlicensed innovation, and sometimes we will want tightly controlled access for specific rights holders
- More intensive use will and should mean more conflicts over spectrum use
- These conflicts should be prevented before the fact by some combination of FCC zoning of compatible uses and industry performance standards
- These conflicts should be addressed after the fact with expedited adjudications and arbitrations, which depend on the creation of the appropriate administrative apparatus (in both private and public institutions)

---

12. Professor, Rutgers University School of Law – Camden. Many thanks to J. Pierre de Vries for organizing the program on radio rights, and to Pierre and Peter Tenhula more generally for stimulating ideas in this area.

13. See Montgomery, *supra* note 1.

14. *Id.*

15. See generally, FCC, *Connecting America: The National Broadband Plan*, March 17, 2010; See Philip J. Weiser & Dale Hatfield, *Spectrum Policy Reform and the Next Frontier of Property Rights*, 15 GEO. MASON L. REV. 549 (2008); Ellen P. Goodman, *Spectrum Rights in the Telecosm to Come*, 41 SAN DIEGO L. REV. 269 (2004).

- Efficient conflict resolution requires that initial entitlements be stated precisely in the license (or license-free allocation) at the outset, and be further articulated in what will be an evolving “common law” allocating responsibilities for mitigating interference
- What the right rule is for allocating responsibilities in any particular spectrum dispute will depend on the kind of services at issue, the relative ability of the parties to address the problem at the receiver or the transmitter, and other public interests (externalities) that may be implicated
- Spectrum use entitlements, both initial and post-dispute, should be made transparent in publicly accessible and user-friendly registries.

While these conclusions have been gestating, battles have played out over the allocation of spectrum for unlicensed and exclusive use, and over the modification of existing licenses to allow for more intensive (and valued) spectrum use.<sup>16</sup> One cannot say that spectrum management has changed much over the past decade or that we have made a great deal of progress in implementing the conclusions stated above. Spectrum management is still pretty much the same as it always has been: highly conservative, protective of incumbents, without clear entitlements and dispute resolution procedures, lacking in the regularity and transparency that would facilitate secondary markets, and, most especially, bogged down in questions of fairness, windfall, strained readings of the public interest, and competitive advantage.

That said, this Commission has made several notable recent decisions to free up spectrum for new uses by modifying existing entitlements and mediating between potential spectrum conflicts. These include the order opening up TV band “white spaces” available for unlicensed fixed and mobile wireless usage,<sup>17</sup> the decision removing obstacles to mobile wireless use of spectrum adjacent to satellite radio,<sup>18</sup> and the proposal to open satellite spectrum to terrestrial wireless use.<sup>19</sup>

16. See, e.g., Thomas W. Hazlett, *Tragedy TV: Rights Fragmentation and the Junk Band Problem*, 53 Ariz. L. J. 83 (2011) (arguing for more licensed spectrum); Kevin Werbach, *The Wasteland: Anticommons, White Spaces, and the Fallacy of Spectrum*, 53 Ariz. L. J. 213 (2011) (arguing for more license-free spectrum); Ellen P. Goodman, *Spectrum Auctions and the Public Interest*, 7 J. TELECOMM. & HIGH TECH. L. 343 (2009) (arguing for spectrum auction design that better accommodates public interest burdens).

17. Unlicensed Operation in the TV Broadcast Bands, *Second Report & Order & Memorandum Opinion & Order*, 23 FCC Rcd. 16807 (Nov. 14, 2008).

18. Amendment of Part 27 of the Commission’s Rules to Govern the Operation of Wireless Communications Services in the 2.3 GHz Band, *Report & Order & Second Report & Order*, FCC 10-82 (May 20, 2010).

19. Fixed and Mobile Services in the Mobile Satellite Service Bands, *Notice of Proposed*

There were some innovations on the spectrum management front here and they are worth building on. The most important decision yet to come will probably concern the reallocation of broadcast spectrum for broadband use.

What can we learn from recent experiences? What would it take to accelerate progress?:

1. *Things take longer when no one can be held accountable for interference.* One of the complications of unlicensed use, however desirable it may be, is that it's hard to assign responsibility for interference. This difficulty buttresses the already existing tendency towards conservative allocations and is one of the reasons the White Spaces decision took so long. Innovative "zoning," revocable certifications and registrations, and a certain amount of reciprocity for interference prevention ease this problem. Underexplored is the role that interference insurance might play.

2. *Failure or inability to deal with the receiver side of the equation produces sub-optimal entitlements.* Whether or not incumbents should have the obligation to improve receiver performance will depend on many factors, including the type of network deployed and the state and pace of technological innovation. Much more clear is that the FCC should have the authority to mandate receiver performance, or to mandate compliance with industry-set standards.

3. *Harmful interference should be a yield sign, not a stop sign.* The FCC continues to use predicted harmful interference as a gatekeeper to spectrum entry.<sup>20</sup> The concept is in effect *both* a tool to define rights (new entrant may not cause harmful interference) *and* a tool to assign liability (new entrant is responsible for harmful interference it does cause). Instead, the notion of harmful interference should be, among other elements, what gives a spectrum user a "cause of action" to seek redress. Whether the harm is actually redressable, and by what means, should be separate questions.

4. *Confusing efficient spectrum use with distributional issues is a recipe for delay.* The public interest in spectrum exploitation and the public (and competitor) interests in preventing licensees from getting windfall benefits are distinct. Whether or not spectrum rights should be expanded, who should get to take advantage of expanded rights, and what they should have to pay for them are all separate issues and should be handled separately, with mechanisms for redistribution of benefits where necessary.

---

*Rulemaking & Notice of Inquiry*, FCC 10-126 (July 15, 2010).

20. 47 C.F.R. § 15.5(b) (2009).

5. *Consideration of values associated with spectrum use other than efficiency is under-developed.* Reallocation of broadcast spectrum in particular will touch on values that are baked into the current allocation, such as universal service, noncommercial set-asides, and distributed access rights. As with distributional issues, these considerations are conceptually separate from efficient spectrum exploitation, but will need to be dealt with.

ECONOMIC PRINCIPLES FOR *EX ANTE* RULES FOR RADIOGREGORY ROSSTON AND SCOTT WALLSTEN<sup>21</sup>

In September 2009, Silicon Flatirons hosted a conference featuring a number of relatively recent case studies of radio regulation and interference.<sup>22</sup> The studies highlighted substantial disputes about rights and responsibilities of radio operation in various bands despite apparently detailed *ex ante* rules by the Federal Communications Commission regarding interference.<sup>23</sup> In each case the parties disagreed about whether the transmitter or the receiver “caused” the interference and if so, whether that party was operating within its rights as defined by the FCC.<sup>24</sup>

These case studies highlight the importance of a regulatory framework that facilitates efficient negotiations between licensees to solve problems by minimizing transactions costs. Such a regulatory framework would start with clear rules and allow parties to negotiate efficiency-enhancing changes to those rules.

*Well-Defined Rights and/or Rules*

Spectrum users are more likely to invest if they understand their own and others’ rights well enough to be reasonably sure their long-lived equipment and infrastructure investments will continue to operate without harmful interference from other users, and that their transmissions will not be shut down because they interfere with other users’ transmissions.

Focusing on emissions into other bands, the cause of harm to adjacent licensees, rather than on transmission power—which is but one potential cause of harm—should increase certainty and help align incentives with minimizing the transaction costs of adapting behavior. If emissions interfere with an adjacent licensee’s transmissions, several solutions not involving the FCC become possible that are not possible,

21. Gregory Rosston is the Deputy Director at the Stanford Institute for Economic Policy Research (SIEPR), and Scott Wallsten is the Vice President for Research and Senior Fellow at the Technology Policy Institute.

22. See Silicon Flatirons Ctr., Telecommunications Regulation in Comparative Perspective, Conference, Sept. 9, 2009, <http://www.silicon-flatirons.org/events.php?id=681> (last visited Jan. 15, 2011).

23. The bands in the case studies included 800 MHz, AWS-BAS, AWS-3 and WCS/DARS.

24. See, e.g., Improving Public Safety Communications in the 800 MHz Band, *Report & Order*, WT Dkt. No. 02-55, 19 FCC Rcd. 14,969 (2004); Lynette Lun, *M2Z asks FCC to reject more AWS-3 interference tests*, FIERCE WIRELESS (Aug. 15, 2008), <http://www.fiercewireless.com/story/m2z-asks-fcc-reject-more-aws-3-interference-tests/2008-08-15>.

or at least not likely, today. For example, the licensee could continue to operate in the same way while the adjacent licensee installs receiver filters to ensure its transmissions still work. Alternatively, if the receiver technology is expensive relative to simply reducing emissions from the transmitter, the adjacent licensee could negotiate with the transmitter to change the technology used. Today, such an outcome is not likely because the parties rely on the FCC to change the rules in favor of one party or another, as well as the difficulty in coming to complete agreements when the FCC has the ability to void the same.<sup>25</sup>

In the spectrum context, the well-known Coase Theorem implies that if transaction costs are zero, or simply less than the transaction costs of other options, parties will agree to an efficient solution to the interference problem.<sup>26</sup> In our example, the transmitter would agree to pay to replace the receiver since that is mutually beneficial. The real world, however, is rife with transactions costs, but policy can improve efficiency by reducing these transactions costs.

Licensees that desire to make trades with neighbors can adapt or make trades to allow for different standards that then become part of their new operating rights. However, to facilitate transactions, the rules need to be set and the FCC must credibly commit to not change those rules in response to political or other pressure. While credible commitments are difficult for regulatory agencies, courts tend to protect against *ex post* rule changes when firms make long-lived investments.<sup>27</sup>

Well-defined rules are important for both licensed and unlicensed bands. Unlicensed bands may require stricter rules because trades of the sort described above could be prohibitively costly given the diffuse and amorphous group of rights holders. Because trading of rights and changing technology is more difficult with unlicensed bands, setting up a rational and clear set of rules in advance is more important for unlicensed bands than for licensed bands.

### *Application to the Case Studies*

One key problem with the historic method of radio regulation based on transmitter power has been its difficulties in dealing with technological change, as exemplified by the dispute between Nextel and the public safety community over the 800 MHz transmissions.<sup>28</sup> The

25. See, e.g., Matthew Lasar, *Wireless Companies Blast Sirius XM in Spectrum Controversy*, RADIO SURVIVOR (Apr. 9, 2010), <http://www.radiosurvivor.com/2010/04/09/wireless-companies-blast-sirius-xm-in-spectrum-controversy>.

26. See Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

27. See, e.g., Penn Cent. Transp. Co. v. City of New York, 438 U.S. 104, 124 (1978); *United States v. Chrysler Corp.*, 158 F.3d 1350 (D.C. Cir. 1998).

28. FCC, *Improving Public Safety Communications in the 800 MHz Band*, Report & Order, WT Dkt. No. 02-55 (July 2004).

FCC wrote rules for 800 MHz private radios with maximum power limits for “high-tower, high-power” sites.<sup>29</sup> The spectrum allocated to “private radio” was nearly identical in its physical properties to the spectrum allocated to cellular service.<sup>30</sup> Nextel (then FleetCall) convinced the FCC to change the private radio rules so that Nextel could function as a CMRS provider and use “low-tower, low-power” cellular architecture.<sup>31</sup> The low power sites did not exceed the power limits of the high power high tower sites, but nonetheless interfered with public safety receivers operating on adjacent channels.<sup>32</sup>

The rules for 800 MHz transmission could have minimized interference between CMRS providers and public safety providers by requiring Nextel to continue to only use high-tower, high-power sites. But that would have disallowed the technological advances and prevented more efficient use of the spectrum.

The FCC could also have allowed the new technology but only if the CMRS licensees negotiated with the public safety entities for the new rights. Flexibility created by clearly defining the rights upfront and allowing changes to the rights upon agreement by the licensees could have led to a mutually agreeable situation.

Finally, and perhaps the best course, would have been to define initially the rights of 800 MHz licensees differently. Rather than designating technology or transmission power, the rights could have explicitly established a maximum level of emissions into adjacent channels. The private radio licensees and the public safety entities would have both known the rules when they began to construct their adjacent systems and acquire their radios. If Nextel had then decided to use a technology that increased emissions into the adjacent channels, it would have known that it would have to negotiate with the public safety agencies if its new transmission method did not comply with the emission limits. If Nextel’s new technology complied with the emissions rules, then the public safety agencies would either have to adapt their receivers or negotiate with Nextel. In both cases, the efficient method of reducing interference would have been selected by negotiation between the parties. Of course, this in part depends on the ability to strike a deal with one or a small number of parties on each side, as transaction costs generally increase with the number of parties needed to reach agreement, all other things being equal.

---

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

## THE NEED FOR WELL-DEFINED YET NON-EXCLUSIVE RADIO OPERATING RIGHTS

MICHAEL CALABRESE<sup>33</sup>

### *Introduction*

As mobile computing becomes ubiquitous, the resulting exponential growth in demand for wireless data transport will strain current spectrum allocation and commercial business models to the breaking point. Silos of exclusively-licensed and lightly-used spectrum will no longer be tolerable. The imperative of increasingly efficient use of spectrum on both an exclusive and shared basis suggests that we need to redefine access rights to spectrum capacity over the next decade to be:

- *More definite:* Rights to transmit *and* levels of protection from third parties (both co-channel and adjacent channel) should be made *explicit* conditions of new and renewed licenses, and subject to secondary-market transactions.
- *More transparent:* The definition of these access rights and the operating parameters of all deployments on a licensed band should be registered in a publicly accessible database that can be used to facilitate decentralized coordination and negotiation, as well as opportunistic access to unused spectrum capacity.
- *More intensive:* Since both shared access to underutilized bands *and* an exponential increase in spectrum re-use will be needed to meet expected consumer data demand, a licensee's affirmative access rights must not preclude the use of any remaining capacity by third parties on a non-interfering basis. Radio rights should conform to a 'use it or share it' ethos.

In short, the FCC needs to return to the unfinished challenge defined by its own 2002 Spectrum Policy Task Force ("SPTF"): To quantify permissible levels of interference on a service-by-band basis.<sup>34</sup> Although Commission staff agreed with a consensus among industry commenters that the "interference temperature" measurements suggested

---

33. Michael Calabrese is a Senior Research Fellow and Director, Wireless Future Program, at the New America Foundation, a non-profit policy institute based in Washington, D.C. Calabrese also currently serves on the U.S. Department of Commerce Spectrum Management Advisory Committee ("CSMAC").

34. See Press Release, FCC, Spectrum Policy Task Force Presents Recommendations for Spectrum Policy Reform (Nov. 7, 2002), [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-228542A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-228542A1.pdf) (listing out the SPTF's recommendations, including the "creation of a quantitative standard for acceptable interference").

by the SPTF appeared unworkable,<sup>35</sup> the concept of quantifying the explicit transmit rights and reception protection that a licensee can count on—on a probabilistic and not absolute basis—would better permit private parties to self-manage issues of interference and shared band access. In contrast, the continued use of a case-by-case, *ex post* adjudication of interference claims will increasingly cause uncertainty, delay, and under-investment.

*Outdated Assumptions of Command & Control Interference Protection*

Today's spectrum allocations and radio operating rights continue to reflect a dichotomy between the relative availability of spectrum and technology that existed during the first half-century or more of spectrum licensing—but which has nearly reversed itself today. When government licensed broadcast radio and television in the first half of the twentieth century, spectrum was plentiful but technology was primitive. Both assignments and rights reflected an industrial policy goal to stimulate the mass-market penetration of very low-cost reception devices (radios, TVs, and later, analog cell phones) in a context of relative spectrum abundance. Since there was spectrum enough to allocate guard bands several times larger than the actual channels in use, the cost of receivers could be minimized and a precedent set that receivers would not be expected to tolerate any degree of interference from other uses.

The policy of protecting receivers from “harmful interference” became simultaneously absolute (rather than probabilistic or contingent) and vague (since it was defined service-by-service, and only *ex post* in reaction to complaints). Moreover, the concept of licensing *exclusive* access to a channel or band presumed that (a) technology and governance rules could not support the shared use of underutilized capacity, except perhaps where there was no protection from interference at all (*viz.*, on designated unlicensed bands); and (b) there were still sufficient allocations and assignments available to meet the public's need for new services and overall communications capacity.<sup>36</sup>

All of these precepts continue to underlie the licensing of radio operating rights—whether to commercial users by the FCC, or to federal users by NTIA—and all are outdated obstacles to an exponential increase in mobile communications capacity.

---

35. FCC, Establishment of an Interference Temperature Metric to Quantify and Manage Interference and to Expand Available Unlicensed Operation in Certain Fixed, Mobile and Satellite Frequency Bands, *Report & Order*, ET Dkt. No. 03-237 (May 4, 2007), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-07-78A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-78A1.pdf).

36. *See, e.g.*, FCC, Wireless Operations in the 3650-3700 MHz Band, *Report & Order & Memorandum Opinion & Order*, ET Dkt. No. 04-151 (Mar. 16, 2005) (suggesting that a non-exclusive licensing approach would accommodate more wireless ISPs by employing technology and coordination that avoids harmful interference).

### *An Updated Radio Rights Regime*

An updated conception of radio operating rights should be based on policy goals that promote pervasive connectivity. It will be far more important to put rules in place that spur innovation and maximize communications capacity than it is to minimize interference per se. Indeed, one of the most oft-quoted passages from Ronald Coase's 1959 article *The Federal Communications Commission* made this point:

It is sometimes implied that the aim of regulation in the radio industry should be to minimize interference. But this would be wrong. The aim should be to maximize output.<sup>37</sup>

Meeting society's demand for mobile communications capacity will require a concept of radio operating rights and governance that may seem contradictory by today's standards. We need to simultaneously make spectrum use rights more like property (more explicit and certain for the period granted) while also making the overall communications capacity of the spectrum less like property (non-exclusive and open for shared access). That is, we need to provide licensees certainty and flexibility concerning their operating rights—thereby facilitating private negotiations and transactions—while also reserving any unused spectrum capacity to the public itself. Since the public interest in government excluding others from a band (i.e., licensing) lies entirely in the use of the spectrum to communicate, it is the licensee's service—viz., its actual use of the band's capacity—that deserves protection, not its non-use.<sup>38</sup>

In practice, I believe this can be achieved by a combination of definitional *and* governance changes:

1. **Define explicit transmit rights and permissible interference on a band-by-service basis.**

For new and renewed licenses, the Commission should make the complete set of transmission rights (e.g., transmit power, out-of-band emissions) explicit. The Commission should also define the level of protection the licensee can expect for its own operations, although this

37. Ronald H. Coase, *The Federal Communications Commission*, 2 J. L. & ECON. 1, 27 (1959).

38. Of course, this follows from both the statutory definition of the FCC's licensing authority, as well as the Commission's fairly recent and explicit rejection of the argument that it does not have the legal right to authorize users of Ultra Wideband devices to emit energy in licensed PCS bands. Rejecting Sprint's claim that its license rights presume exclusive rights to emit on the band, the Commission firmly stated that "spectrum is not, and has never been, exclusive to Sprint or to any other licensee or user." Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems, *First Report & Order*, FCC Rcd. 10,505, ¶ 271 (2002).

should be defined in probabilistic rather than absolute terms. These rights, when first defined, would need to be defined service-by-band and as consistent as possible with neighboring adjacent- and co-channel licensees.

## 2. Combine explicit rights and actual operating parameters of licensees in a public database.

If key policy goals are to maximize useable spectrum capacity and facilitate innovation, then we should want complete transparency into both what licensees have a right to do and *what they actually are doing*. This enables other licensees to design their systems, to change the use of a band, or to attempt to coordinate and/or negotiate with other users. It also enables other potential users to employ dynamic spectrum access technologies or protocols to make use of *unused capacity* without causing harmful interference. Depending on the band, this dynamic access could be based on secondary market transactions, or it could be opportunistic and/or unlicensed. Access to any band with a primary user must be conditional; but a centralized, online information registry “enables secondary users to execute more aggressive spectrum access algorithms at acceptably low risk.”<sup>39</sup>

The current opaque and uncertain definition of rights for incumbents and potential entrants alike deters both innovation and more intensive and efficient use of the public’s spectrum resource. It is critical to keep in mind that spectrum is an infinitely-renewable public resource, and from second-to-second any capacity that goes unused is wasted. A more definite, transparent, and explicitly non-exclusive definition of spectrum use rights on a band-by-band basis will be critical to supplying the capacity for pervasive connectivity.

---

39. John M. Chapin & William H. Lehr, *The Path to Market Success for Dynamic Spectrum Access Technology*, IEEE COMM’NS MAG., May 2007, at 96, 100. Australia established a centralized online device database along these lines as part of its 1997 adoption of Space-Centric Management as a tool to define a complete set of explicit transmit rights for all new licenses to encourage certainty and industry self-regulation. See Michael Whittaker, *Authorising Dynamic Spectrum Access Under Space-Centric Management*, FUTURESPEACE (Feb. 2009), [http://www.futurepace.com.au/\\_lib/pdf/DSA.pdf](http://www.futurepace.com.au/_lib/pdf/DSA.pdf).

FORWARD-LOOKING INTERFERENCE REGULATION<sup>40</sup>EVAN KWEREL AND JOHN WILLIAMS<sup>41</sup>

To facilitate the transition of spectrum to its highest valued use under a flexible licensing regime, we propose that the FCC revisit its general policy of providing incumbents (those licensed first) protection against any interference resulting from subsequent rule changes. It is well known that limiting spectrum licensees to providing specific services using specific technologies (“command and control”) can seriously retard the adoption of new highly valuable technologies, such as cellular telephones.<sup>42</sup> The FCC has recognized this and since the early 1990s has been providing for service and technological flexibility for most newly allocated bands.<sup>43</sup>

What is less well known is that the FCC’s sequential approach to accommodating change coupled with its interference protection policy toward incumbent uses can also be detrimental to putting spectrum to its highest value use. When considering a new allocation or request for a change in interference rules, the Commission generally considers one item at a time assuming everything else will remain as is.

Rules protecting the adjacent band incumbents are based on a long tradition in spectrum management that incumbents have the right to virtually absolute protection from interference from new users.<sup>44</sup> Because of this, incumbents generally feel little or no pressure from the regulator to improve filtering or implement other additional mitigation measures. The additional limits imposed on the flexible use band are based on an interference model using the incumbent’s system parameters and

---

40. A more detailed exposition can be found at Position Papers, *The Unfinished Radio Revolution: New Approaches to Handling Wireless Interference*, SILICON FLATIRONS CTR., Nov. 12, 2010, <http://www.silicon-flatirons.org/documents/conferences/2010.11.12-862/Compendium.pdf>.

41. Evan Kwerel is a Senior Economic Advisor at the FCC. John Williams is a consultant at Ambit. The opinions expressed in this paper are those of the authors and do not necessarily represent the views of the FCC or any other members of its staff.

42. See generally Coase, *supra* note 37; see also M. CAVE ET AL., *ESSENTIALS OF MODERN SPECTRUM MANAGEMENT* 4-8 (2007).

43. See *Personal Communications Services*, 47 C.F.R. pt. 24.

44. Incumbent users are generally protected from harmful interference with no time limit on such protection. Harmful interference is defined in 47 C.F.R. § 2.1 as interference “which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service.” The only exception I can think of is where incumbents are being cleared from a band that is being repurposed for flexible use. For example, incumbent point-to-point systems in the PCS band were protected for a period of time, during which time they could negotiate a premium payment to clear, after which time they were required to vacate as long as the new PCS licensee covered the actual cost of a replacement service. To my knowledge, the FCC has never sunsetted restrictions imposed to protect adjacent band incumbents.

parameters of “expected” use for the flexible licensees.<sup>45</sup> This often results in additional power and other restrictions on the flexible use band that are significantly more stringent than those that apply between flexible use bands, with the effect of reducing the functionality of that band.<sup>46</sup>

*Future allocations should self-protect against projected adjacent band interference*

When a new allocation is made and there are no incumbents in an adjacent band or the band is lightly used under a command/control type allocation, the FCC should require that licensees self protect against interference exposure from adjacent band(s), *assuming* that those bands would be licensed under the flexible use model. We propose that the interference rules and assumptions protecting the new allocation from interference from the adjacent bands be designed in such a way as to preserve as much as possible the full potential of the adjacent bands for future use under a flexible licensing regime. So, if the adjacent band has a high potential for transition to flexible use, it would not be subjected to technical limits (power, permissible classes of stations, etc) more stringent than would normally apply between adjacent flexible use bands. Since this policy may, in some cases, raise the cost of a new allocation, it should be accompanied with a commitment by the FCC to actually transition the adjacent bands to a flexible regime.

This would internalize the total spectrum cost of accommodating the new use rather than passing some or most of that cost off to someone else. It would also provide better incentives to build more interference-robust systems upfront when it is most efficient to do so. It would also make transparent the opportunity cost of any new allocation in terms of its impact on the spectrum whereas current policy which assumes an adjacent band that is now sparsely populated would remain so hides the full cost of a new allocation.

*Adjacent band interference protection for incumbents should not be static*

When the FCC establishes a new flexible use allocation, power and other restrictions are often imposed on that band to protect incumbents in adjacent bands.<sup>47</sup> These restrictions can be more stringent than would normally apply between flexible-use bands.<sup>48</sup> While such restrictions may

---

45. Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands, *Report & Order*, FCC 03-251, ¶ 87, 112-131 (Nov. 25, 2003), *available at* [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-03-251A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-251A1.pdf) (describing interference protections for incumbents adjacent to the AWS-1 bands).

46. *Id.*

47. *Id.*

48. *Id.*

be equitable to protect the investments of incumbents, they can greatly reduce the potential value of the newly allocated band. Under these static protection policies, incumbents have little incentive to implement even low cost measures to protect themselves since the benefits would go to someone else. Bargaining between new licensees and incumbents in adjacent bands is also generally ineffective due to high transaction costs. The resulting economic loss worsens over time as the value of adjacent spectrum increases and the cost of mitigation technology decreases.

To address this, we propose that when a new flexible use allocation is made and there are incumbents in an adjacent band, restrictions imposed on the new allocation to protect adjacent incumbents against interference be reduced over time to mirror the same protections provided between adjacent flexible use bands.

We would also extend this approach retroactively within the valuable 300 to 3000 MHz range to restore functionality to bands that are good candidates for flexible use. Any stringent power or other restrictions that currently apply to those bands designed to protect adjacent band incumbents (limited to bands within the FCC's jurisdiction) would be reduced to the same level as applies between flexible use bands. Again, this would be accompanied by a commitment by the FCC to actually transition those candidate bands to flexible use so that the benefits can be realized.

#### *Market failures justifying changing interference regulation*

Why not rely on the market to efficiently resolve these interference problems? What are the market failures that would justify such a policy change? First, when not all rights have been assigned there is nobody to negotiate with. When an adjacent band is not licensed or not all the rights are assigned (*e.g.*, bands with traditional services such as broadcasting where there is "white space") a new licensee in an adjacent band has no one to negotiate with to design a system that minimizes the total cost of interference. You can't negotiate with future licensees. The direct solution would be to assign all rights. But when most of the spectrum is occupied with traditionally licensed users this is difficult. Kwerel and Williams (2002) address this issue.<sup>49</sup>

Second, even when most rights have been assigned, but many licensees must agree to negotiate a change in the rules, holdout problems, free riding, and generally high transactions costs may prevent achievement of a deal that potentially could make all parties better off.

---

49. See Evan Kwerel & John Williams, *A Proposal for a Rapid Transition to Market Allocation of Spectrum* (FCC Office of Plans and Policy, Working Paper No. 38. Nov. 2002).

## THE THREE PS: A RESULTING ENERGY APPROACH TO RADIO OPERATING RIGHTS<sup>50</sup>

J. PIERRE DE VRIES<sup>51</sup> AND KALEB A. SIEH<sup>52</sup>

The radio revolution is incomplete. The shift from “command and control” radio licensing to a more hands-off regime of flexible-use auctioned licenses and unlicensed operation is well under way, but the vital question of how radio operating rights should be defined, assigned and enforced in order to resolve interference disputes and obtain the maximum benefit from wireless operations remains largely unanswered.

The ambiguous definition of rights is a long-standing problem. For example, the FCC’s 2002 Spectrum Policy Task Force noted a widespread sentiment that “the Commission’s most difficult, controversial, and unsatisfactorily resolved cases have resulted from situations in which the extent of an incumbent’s spectrum rights and interference rights, and its limitation on impacting other bands or users, were not clearly understood by the incumbent, by a new service provider, and even by this Commission.”<sup>53</sup>

A review of U.S. interference conflicts stemming from unclear cross-channel rights reveals instances where: two (or more) licensees are both operating within their licenses but unable to operate concurrently (800 MHz);<sup>54</sup> the FCC changes the license rights after auction but before renewal (WCS/SDARS);<sup>55</sup> lack of clarity concerning cross-channel protections leads to protracted proceedings (AWS-3);<sup>56</sup> and a new

50. A more detailed exposition can be found at J. Pierre de Vries & Kaleb A. Sieh, *Increasing Concurrent Operation by Unambiguously Defining and Delegating Radio Rights* (Oct. 6, 2010) <http://papers.ssrn.com/abstract=1704194>.

51. Senior Adjunct Fellow, Silicon Flatirons Center, University of Colorado, Boulder.

52. Research Fellow, Silicon Flatirons Center, University of Colorado, Boulder.

53. FCC SPECTRUM POLICY TASK FORCE, REPORT OF THE SPECTRUM RIGHTS AND RESPONSIBILITIES WORKING GROUP (2002), *available at* [www.fcc.gov/sptf/files/SRRWGFfinalReport.doc](http://www.fcc.gov/sptf/files/SRRWGFfinalReport.doc).

54. Improving Public Safety Communications in the 800 MHz Band, *Report & Order, Fifth Report & Order, Fourth Memorandum Opinion & Order, & Order*, WT Dkt. 02-55, ¶ 13, 15 (July 2004).

55. Amendment of Part 27 of the Commission’s Rules to Govern the Operation of Wireless Communications Services in the 2.3 GHz Band, *Report and Order and Second Report and Order*, WT Dkt. No. 07-293, ¶ 5 (May 2010).

56. *See* M2Z Networks, Inc., Application for License and Authority to Provide National Broadband Radio Service in the 2155-2175 MHz Band (2006), *available at* <http://fjallfoss.fcc.gov/ecfs/document/view?id=6518725080>; *see also* PR Newswire, *FCC Terminates AWS-3 Rulemaking to Auction Spectrum with Free Broadband Requirement; Breaks National Broadband Plan Commitment*, Sept. 1, 2010, <http://www.prnewswire.com/news-releases/fcc-terminates-aws-3-rulemaking-to-auction-spectrum-with-free-broadband-requirement-breaks-national-broadband-plan-commitment-101967093.html> (last visited Jan. 11, 2011).

entrant discovers an unforeseen need to remedy harm to adjacent channel incumbents (AWS-1/BAS).<sup>57</sup> Inter-operator conflict is greatest across boundaries between different service types and the increasing diversity of radio uses and users, as well as the need to pack operations ever closer together, will only serve to amplify the problem.

Current radio operating rights are uncertain due to: the use of the harmful interference criterion;<sup>58</sup> technical parameters that do not define the bounds of allowed operation objectively;<sup>59</sup> the regulator's willingness to alter operating rights at any time during the term of the license;<sup>60</sup> and ineffective delegation to operators of the means and incentives to negotiate bilateral resolutions.<sup>61</sup> This has led to protracted conflicts and unexpected costs, which in turn inhibit innovation and investment.

Scholars seeking quick ways to build coherent and efficient property rights systems for developing countries have derived best practices and key elements from what they consider successful property rights systems. According to one analysis, a successful real property rights system should: (1) capture, describe, and organize the most economically and socially useful aspects of an asset; (2) have formal rules for the description and organization of this information; (3) preserve the information in a recording system; and (4) be tilted towards protecting transactions.<sup>62</sup> Importantly, the rules should be clear and enforced in an efficient and predictable manner.

In this spirit, our approach is based on three principles: (1) aim regulation at maximizing concurrent operation, not minimizing harmful interference; (2) delegate management of interference to operators; and (3) define, assign and enforce entitlements in a way that facilitates transactions.

57. See *The Society for Broadcast Engineers, Petition for Reconsideration*, WT Dkt. No. 02-353, ¶ 6 (Mar. 8, 2007); see also 47 C.F.R. § 27.1133 (2003).

58. See 47 C.F.R. § 2.102(f) (2003); see also 47 C.F.R. § 27.1133.

59. FCC SPECTRUM POLICY TASK FORCE, *supra* note 53 (noting that "the Commission's most difficult, controversial, and unsatisfactorily resolved cases have resulted from situations in which the extent of an incumbent's spectrum rights and interference rights, and its limitation on impacting other bands or users, were not clearly understood by the incumbent, by a new service provider, and even by this Commission").

60. FCC, Amendment of Part 27 of the Commission's Rules to Govern the Operation of Wireless Communications Services in the 2.3 GHz Band, *Report & Order & Second Report & Order*, WT Dkt. No. 07-293, ¶160.

61. See J. Pierre de Vries & Kaleb A. Sieh, *The Three Ps: A Resulting Energy Approach That Increases Concurrent Operation By Delegating the Optimization of Operating Rights*, 15 (Oct. 2010), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1704194](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1704194).

62. HERNANDO DE SOTO, *THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE* (2000); see also, Hernando de Soto, *Mystery of Capital*, 38 FINANCE & DEV. no. 1, Mar. 2001, at 29.

*Define radio operating rights through probabilistic permissions and protections, without reference to harmful interference*

We propose that operating rights should be articulated using probabilistic transmission permissions and reception protections (“The Three Ps”). Since the radio propagation environment changes constantly, parameter values should be defined probabilistically as a percentage of times and locations. Transmission permissions should be based on resulting field strength over a range of locations and frequencies, rather than the radiated power at a transmitter. Reception protections should state the maximum outside electromagnetic energy an operator can expect over a location/frequency profile; protection levels are an undertaking by the regulator to implement these ceilings when making other allocations, but importantly do not form an entitlement against other, existing operators. This formulation of operating rights does not require a definition of harmful interference. Quantifying and addressing harmful interference remains a very important topic, but is delegated to operators and, should negotiation fail, adjudicators.

*Limit the ability of the rule maker to adjust rights*

Since the initial entitlement point is unlikely to be optimal, or remain optimal for very long, the regulator should do all it can to facilitate adjustment of rights after the fact. In this process, the number of parties to a negotiation should be limited, both through rights assignments that minimize the number of recipients as much as possible, and by the regulator enabling direct bargaining between the parties. The regulator should stipulate the remedies that attach to an entitlement (i.e. injunctions or damages) when it is issued, and not decide such things *post hoc* in its capacity as an adjudicator. The regulator should clearly separate rulemaking, where it plays an essential role in defining entitlements, from the enforcement/remedy phase where its role, if a court is not available, should be limited to adjudication on the basis of existing rules. Notably, the regulator should refrain, to the extent possible, from rulemaking when acting as an adjudicator.

*Record entitlements in a public registry*

In the radio license context, the full and complete description of every entitlement—including owner, Three P operating parameters, fixed station locations if applicable, and waivers if any—should be recorded in a public registry. And finally, the regulator should refrain from changing the rules, or adding new ones, in the middle of the game. After defining operating rights, parameters, and remedies in a license, the regulator should leave entitlements unchanged until renewal. However, those same

rights, parameters and remedies should be allowed to adjust through negotiation between operators.

The fruits of the radio regulation revolution can thus be gained by an objective articulation of the rights in an operating license, and the effective delegation of negotiation and dispute resolution to operators.

## SPECTRUM “PROPERTY RIGHTS” AND THE DOCTRINE OF ADVERSE POSSESSION

HAROLD FELD\*

Since the introduction of auctions and the wider acceptance of secondary market transactions, those favoring a market-based approach for spectrum access<sup>63</sup> have focused on the definition of spectrum property rights as the means to maximize the efficient development of spectrum.<sup>64</sup> But even if one accepts the basic premise that defined and easily traded spectrum property rights enhance overall development of wireless services and technologies, it does not follow that simply defining and enforcing these rights will resolve all problems that will emerge. The doctrines of real property include significant exceptions based on common good and common reliance,<sup>65</sup> and one should expect similar exceptions to emerge for similar reasons in spectrum policy.

Of particular relevance, the doctrine of “adverse possession” provides circumstances under which the right of a property holder yields to a squatter.<sup>66</sup> This exception amounts to a recognition by the law that at a certain threshold the rights of the owner yield to the reliance interest of the community generally and the “facts on the ground.” By embracing, defining, and limiting this narrow exception to the right of an owner to expel a trespasser, property law creates a necessary safety valve for dealing with extraordinary circumstances while simultaneously preserving the stability and predictability that make property rights useful.

This basic concept has important lessons for spectrum policy and definitions of spectrum property rights.

---

\* Legal Director of Public Knowledge, <http://www.publicknowledge.org>.

63. See Coase, *supra* note 37.

64. See SPECTRUM POLICY TASK FORCE REPORT SEEKS PUBLIC COMMENT ON ISSUES RELATED TO COMMISSION’S SPECTRUM POLICIES PUBLIC NOTICE, 17 FCC Rcd. 10560 (June 6, 2002); see also Phil Weiser & Dale Hatfield, *Spectrum Policy Reform and the Next Frontier of Property Rights*, 60 GEO. MASON L. REV. 549 (2008) [hereinafter *Spectrum Policy Reform*] (describing difficulty in establishing clear definition of spectrum property rights but arguing for necessity of overcoming difficulties).

65. For example, the government may force a sale of the property at fair market value for public purposes. See *Kelo v. City of New London*, 545 U.S. 469 (2005). The doctrine of nuisance constrains the ability of a landowner from certain uses of the land that would interfere with a neighbor’s quiet enjoyment. Further, in cases where new development of land may deprive the owner of a neighboring plot ready access, the common law typically required the property owner to provide to his neighbor an easement for access and egress.

66. See BLACK’S LAW DICTIONARY 59 (8th ed. 2004) (defining adverse possession).

*Examples of Difficulties Despite Clear Definitions of Spectrum Rights: The 800 MHz Rebanding and the 700 MHz Wireless Microphone Order*

Two examples illustrate how exceptional circumstances can arise and the value of defining a set of principles that both cabin the exception and provide a roadmap for resolution.

In 2004, the FCC resolved a long-standing interference dispute between Nextel (later Sprint Nextel) and the public safety community resulting from the interference to public safety systems caused by Nextel's commercial operations in the 800 MHz band.<sup>67</sup> Despite clear definitions of rights and FCC support for market-based resolution of interference complaints, the problem eventually grew to involve millions of subscribers and thousands of public safety systems.<sup>68</sup> After a lengthy proceeding, the FCC required Sprint Nextel to transfer its operations to a different band.<sup>69</sup>

It is tempting to blame the FCC for its failure to enforce the "property rights" of public safety licensees by requiring immediate shut down of Nextel's systems. But the true nature of the problem only became clear when Nextel operations expanded dramatically, so that shutting it down would have imposed significant costs on millions of subscribers. At the same time, FCC rules and the public interest required that the FCC protect public safety licensees from Nextel's "trespass." The FCC therefore imposed a solution that had nothing to do with the definition or enforcement of property rights and everything to do with finding a working balance among the competing interests.

The FCC found itself faced with a similar situation with regard to the illegal use of wireless microphones in the broadcast television bands.<sup>70</sup> Since the 1970s, the FCC had permitted only television and cable program producers (and a limited number of others) to operate in these bands.<sup>71</sup> Unfortunately, manufacturers and retailers had sold hundreds of thousands (if not more) of wireless microphones operating on the 700 MHz band to numerous unauthorized venues ranging from Broadway theaters to megachurches to karaoke bars.<sup>72</sup> Because these unauthorized users did not cause interference with broadcast television, their increasing

67. Improving Public Safety Communications in the 800 MHz Band, *Fifth Report & Order, Fourth Memorandum Opinion & Order*, 19 FCC Rcd. 14,969 (2004). The history is summarized in ¶¶ 13-14, 36-46.

68. *Id.*

69. *Id.* ¶¶ 217-231.

70. See generally, FCC, Revisions to Rules Authorizing the Operation of Low Power Auxiliary Stations in the 698-806 MHz Band, *Order*, 25 FCC Rcd. 643 (Jan. 15, 2010) [hereinafter *Wireless Microphone Order*], available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DA-10-92A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-10-92A1.pdf).

71. See 47 C.F.R. § 74.832 (2005).

72. See generally, *Wireless Microphone Order*, *supra* note 70.

numbers went unnoticed until the FCC began a proceeding to authorize unlicensed use of unassigned television channels for broadband (the “broadcast white spaces”) and to reallocate the 700 MHz band to commercial and public safety licensees as part of the transition to digital television.<sup>73</sup>

Wireless microphone users protested against their displacement from the 700 MHz band and potential interference from newly authorized white space devices.<sup>74</sup> Under the rights defined by the FCC’s rules, the FCC should have simply ordered the wireless microphone “spectrum squatters” to cease operation or, at a minimum, suffer interference from authorized systems.<sup>75</sup> After two years, however, the FCC reluctantly concluded that the squatters had acquired an equity interest in continued operation despite their status as illegal operators.<sup>76</sup> Although proceedings continue, the FCC adopted a general solution that retroactively legalized the wireless microphone operators and allocated them channels off the 700 MHz band.<sup>77</sup>

### *Some Basic Lessons*

In both these cases there was no doubt as to the “correct” answer under the existing definition of rights, and no further definition of rights would have prevented the situation from occurring. Nor as a practical matter could the FCC be expected to have prevented the problem through enforcement. By the time the situation reached a point where swift, widespread enforcement was necessary, it was too late.

Recognition that exceptional cases arise combined with a set of guiding principles would have allowed the FCC to solve these use conflicts in a straightforward manner, preventing years of delay. Instead, the FCC found itself confronted with an apparently irreconcilable conflict between enforcing the rights of the licensees and the practical consequences of such an action. As a result, it dealt with each situation as a unique circumstance requiring years to develop a solution.

Clear definitions of licensee rights, and access to swift enforcement mechanisms, will benefit all users of wireless by enhancing the ability of licensees to engage in efficient transactions. But situations will continue to arise, as they do in the real property context, where the rights of licensees must yield to other considerations. The law of real property deals with these situations by addressing them in a straightforward manner through mechanisms like the doctrine of adverse possession. Spectrum policy must learn to do the same.

---

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

HOW SHOULD RADIO OPERATING RIGHTS BE DEFINED, ASSIGNED,  
AND ENFORCED IN ORDER TO OBTAIN THE MAXIMUM BENEFIT  
FROM WIRELESS OPERATIONS?

BRUCE JACOBS<sup>78</sup>

I agree completely with the premise of J. Pierre de Vries's paper about the benefits of clarifying radio operating rights.<sup>79</sup> As someone who has been working on these issues since 1982 and has been advocating and negotiating on behalf of proponents of many new services, including Mobile Satellite Service (including its Ancillary Terrestrial Component), Satellite Radio (including terrestrial repeaters), Broadband Radio Service, Broadband over Powerline, and several others unfortunately too obscure to mention, I have seen firsthand the frustration with the delay that characterizes the current regulatory process of defining and redefining rights. Over the years, the process has improved, but for more optimal technology development and capital investment, we should continue to strive for a more predictable jurisprudence that can minimize the delay inherent in relatively *ad hoc* processes. Engineers need to know what filters must be developed and what power levels they can rely on in a deployment design and business people who are interested in investing or doing deals must be in a better position to judge their risks.

Ellen Goodman's San Diego Law Review article makes the excellent point that we cannot avoid defining such rights, regardless of whether the overall regime is one of command-and-control, shared access, exclusive use, or something else, and regardless of whether the remedy is injunctive relief or damages.<sup>80</sup> In any of these cases, harmful interference needs to be defined, including how it is to be measured.

I do not want to minimize the difficulty of the task. Let's take Pierre's reasonable proposal that rights be established based on field strength spectral density at X% of locations, Y% of the time.<sup>81</sup> How is that energy going to be measured? Ellen's article points out that there is no commonly agreed way to measure emissions levels in a given geographic area, which is understandable given the complexity. Do you use actual field measurements or a predictive model? If you take measurements, what antenna and receiver do you use? If you use a predictive model, which model is appropriate? What clutter database do you use? What separation distance should be assumed? What height should be used? In a mobile environment, where interference is often

---

78. Partner, Pilsbury Winthrop Shaw Pittman.

79. See *supra* pp. 519-22.

80. See Goodman, *supra* note 15.

81. See *supra* pp. 519-22.

fleeting, what probabilistic model should be used? The answers to each of these questions can have an enormous impact on the results and each needs to be addressed in order to establish the certainty that we are looking for.

The FCC has had good reason to prefer a more *ad hoc* approach, given the dynamic nature of technology and the varying policy implications of each case. For instance, adoption of Pierre's suggested regime would involve an enormous potential reallocation of value depending on the level of protection (i.e. field strength spectral density at X% of locations, Y% of the time) set for the first time for existing licensees. Given the billions of dollars invested in legacy systems deployed under the current regime, those decisions would be enormously controversial and the potential transition quite costly. Moreover, would the new level be uniform for all services or would it account for differences in real or perceived protection levels? Does spectrum used for satellite services that necessarily deploy more sensitive receivers have the same protection as that used for terrestrial fixed services that typically operate with more link margin? How about services like Radio Astronomy? The enormity of the task is obvious.

Given these challenges, it is not clear to me what is the most realistic way to make either incremental or more radical improvement. I like Pierre's suggestion that the FCC try to establish a protection level for new licensees (along with an approach to measurement), in which case there will not be the same transition costs and potential reallocation of value as there would be for legacy systems. I also would encourage the FCC, despite the complexity of the task and the potential limits on its flexibility, to consider attempting to generalize the principles and criteria it uses to set the protection level and measurement approach, to foster a more transparent and predictable set of rights for future proceedings. One starting point might be a compilation of the existing body of FCC decisions defining harmful interference and how it is measured, to see what lessons they offer on defining and measuring harmful interference. The FCC's past decisions, although not always as transparent as they might be (at least to us non-engineers), may provide a valuable starting point for developing a more predictable jurisprudence and for advancing the process of establishing greater predictability. This and other aspects of the effort to develop such a jurisprudence might be undertaken with the assistance of, as Mike Marcus suggests, the National Academy of Sciences, or of interested parties with something to gain from greater predictability.

## DEFINING RADIO RIGHTS: THEORY AND PRACTICE

CHARLA M. RATH<sup>82</sup>

For years, academics and other researchers have been struggling with the question of how to define radio operating rights. As demand for spectrum grows, and as this conference demonstrates, many are seeking to develop a more robust theoretical framework for defining, assigning and enforcing such rights. It is equally important, however, to investigate current practice with respect to interference rights and consider how licensees resolve interference scenarios in today's marketplace. A framework cannot rely solely on analysis of the intractable large-scale issues such as the competing interference claims often contained in de novo spectrum allocation proceedings, but should explore how licensees, with the flexibility to do so, trade rights and resolve innumerable local interference issues.

To that end, what is it like to provide an itinerant, dynamic consumer service that operates 24/7, reaches 289 million Americans and depends on a difficult to manage resource that is federally regulated? Verizon Wireless has nearly 100 million customers, more than 1500 mobile licenses (not to mention thousands more microwave licenses), tens of thousands of cell sites transmitting on several frequencies and tens of thousands of miles of RF borders and boundaries.<sup>83</sup> In order to constantly improve our service to the customer, and because interference is a costly drag on our network's capabilities, we must deal with issues of rights and interference on a daily basis. It is critical to our business that we are able to negotiate and resolve quickly most, if not all, rights and interference issues without seeking intervention or assistance of the Federal Communications Commission.

There has been some discussion in the literature as to the usefulness of applying the lessons learned about these kinds of negotiations to the larger question of defining interference rights.<sup>84</sup> It is not practical within

82. Vice President – Public Policy, Verizon.

83. Press Release, Verizon, Verizon Reports Strong 4Q and Year-End 2010 Results, Highlighted by Cash Flow, Wireless and FIOS Growth (Jan. 25, 2011), [http://www22.verizon.com/investor/newsatglance/news.htm?dID=6303&dDocName=NEWS\\_1107&xCategory=News; Spectrum Dashboard, REBOOT.FCC.GOV, http://reboot.fcc.gov/reform/systems/spectrum-dashboard](http://www22.verizon.com/investor/newsatglance/news.htm?dID=6303&dDocName=NEWS_1107&xCategory=News; Spectrum Dashboard, REBOOT.FCC.GOV, http://reboot.fcc.gov/reform/systems/spectrum-dashboard) (last visited May 25, 2011); see also *FCC Universal Licensing System*, FCC, <http://wireless.fcc.gov/uls> (last visited May 25, 2011); Ex Parte Letter from Verizon Wireless to FCC, EB Dkt. No. 06-119 and WC Dkt. No. 06-63 (filed Sept. 4, 2007).

84. See, e.g., *Spectrum Policy Reform*, supra note 64; Thomas W. Hazlett, *A Law & Economics Approach to Spectrum Property Rights: A Response to Weiser and Hatfield*, 15 GEO. MASON L. REV. 975 (2008). See also Philip J. Weiser & Dale N. Hatfield, *Property Rights in Spectrum: A Reply to Hazlett*, 15 GEO. MASON L. REV. 1025 (2008); Thomas W. Hazlett, *A Rejoinder to Weiser and Hatfield on Spectrum Rights*, 15 GEO. MASON L. REV. 1031 (2008).

the limited scope of this short paper to consider the details of wireless carriers' rights and experience with interference management. Two areas illustrate, however, why any discussion of radio operating rights can benefit from a better understanding of licensees' market based approach to rights and interference management: first, where the individual licensee has clear, enforceable rights and is permitted to negotiate extensions of these rights and second, where the class of licensees has enforceable rights, but needs additional regulatory clarity in order to resolve interference issues.

*Clear, Enforceable, Negotiable Rights - FCC Rules Allow for Private Agreements*

Unlike most radio services, the rules governing mobile wireless carriers permit private rights negotiations. Under the Commission's PCS rules (and AWS and 700 MHz rules) parties can agree to a higher field strength than is outlined in the rules.<sup>85</sup> Commission rules also permit cellular licensees to negotiate service area boundary extensions agreements with neighboring licensees.<sup>86</sup> Wireless carriers' thousands of licenses and thousands of miles of adjacent and co-channel boundaries create a laboratory for evaluating whether this successful approach to interference "rights" negotiations is pertinent to a larger radio operating rights framework.

Under current rules, licensees negotiate to extend rights into each others' licensed spectrum on a daily basis. These are not massive, one-time negotiations between companies, but involve hundreds of individual negotiations between companies' engineers who are tasked with the day-to-day operations of the network. And, although mobile wireless licensees are, for the most part, "stable and 'repeat players,'"<sup>87</sup> this does not mean interests are always aligned or that licensees always get what they want or need. Indeed, not all negotiations are symmetrical or mutual—in our case, we attempt reciprocity when we seek to extend RF borders, but these negotiations can be difficult and carriers (including Verizon Wireless) do not always achieve their goals. That said, because the rights of both licensees are clear, there is no benefit to seeking regulatory redress. Instead, we manage the process in the market and

---

85. 47 C.F.R. § 24.236 (1994). The Commission's Part 27 rules, which cover both AWS 1 and 700 MHz spectrum licenses, also permit these kinds of field strength agreements. 47 C.F.R. § 27.55(a)(2008).

86. 47 C.F.R. § 22.912 (2003). Unlike PCS, new cellular agreements that extend the boundaries of a cellular licensee's coverage are considered a major modification to the license and thus must be approved by the FCC. Moreover, these agreements are more cumbersome than the PCS field strength agreements in that they often need to be renegotiated when the licensee changes technology.

87. *Spectrum Policy Reform*, *supra* note 64, at 589.

look to other ways to gain the rights to spectrum we need to operate—typically through spectrum purchase or lease.

*Unauthorized Operator-to-Licensee Interference—Need for Additional Enforcement Assistance*

Licensees also deal with thousands of instances of interference from unauthorized operations each year. Again, licensees' efforts to resolve these issues are very much local and generally do not involve the FCC. If we can locate the source of harmful interference, we can often work with the owner of the property or transmitter to address the problem. However, some cases may require FCC intervention, such as in 2006 when a signal booster installed in a Manhattan office building interfered with about 200 Verizon Wireless cell sites in New York and New Jersey.<sup>88</sup> Although most instances of booster interference are smaller in scale, they still can be difficult to resolve—the source may be nearly impossible to identify if installed in a moving vehicle or boat for example. Interference from these and other sources costs carriers thousands of hours to investigate and, where possible, to resolve. In the case of boosters licensees are not seeking individual relief, but are asking the Commission to confirm licensee rights and take a strong stance on the marketing of these devices, so that licensees can address these interference issues more forcefully in the marketplace.<sup>89</sup>

*Final Thought*

Getting the right theoretical framework to define radio operating rights is important, but the exercise must be informed by the experience licensees have gained resolving interference issues in an increasingly complex and market-oriented RF environment.

---

88. Radio signal boosters, repeaters or amplifiers that are marketed and used without a wireless carrier's authorization are a growing and serious cause of harmful interference to wireless networks.

89. See Comments and Reply Comments of CTIA in *Wireless Telecommunications Bureau Seeks Comment on Petitions Regarding the Use of Signal Boosters and Other Signal Amplification Techniques Used with Wireless Services*, WT Dkt. No. 10-4; DA 10-14 (Jan. 6, 2010); see also Comments and Reply Comments of Verizon Wireless. Specifically, Verizon Wireless has asked that the Commission (1) confirm that signal boosters cannot be operated without a license or licensee approval, and (2) declare that signal boosters cannot be sold to entities not authorized to operate them.

# THE ROLE OF NON-UTILITY SERVICE PROVIDERS IN SMART GRID DEVELOPMENT: SHOULD THEY BE REGULATED, AND IF SO, WHO CAN REGULATE THEM?

ANDREAS S. V. WOKUTCH\*

|  |     |
|--|-----|
| INTRODUCTION.....  | 532 |
| I. OVERVIEW OF SMART GRID DEVELOPMENT .....  | 533 |
| II. WHY NUSP-CONSUMER INTERACTIONS SHOULD BE REGULATED.....  | 534 |
| <i>A. What are NUSPs and How Do They Interact with Consumers?</i> .....  | 535 |
| <i>B. Cyber Security and Privacy Concerns of NUSP-Consumer Interactions</i> .....                                | 538 |
| 1. Cyber Security Concerns .....   | 538 |
| 2. Privacy Concerns .....  | 543 |
| III. WHAT ENTITY HAS AUTHORITY TO REGULATE NUSP-CONSUMER INTERACTIONS?.....                                      | 544 |
| <i>A. No Entity has Authority to Regulate NUSP-Consumer Cyber Security Concerns</i> .....                        | 545 |
| 1. The FERC—Partial and Inadequate Regulatory Authority.....   | 545 |
| 2. PUCs—No Authority to Regulate .....   | 552 |
| 3. The DOE—No Authority to Regulate .....  | 555 |
| 4. The FCC—Perhaps Able But Unlikely to Regulate ....  | 557 |
| 5. The DHS—No Authority to Regulate.....   | 558 |
| <i>B. Only PUCs or the FTC’s State Analogues Have Authority to Regulate NUSP-Consumer Privacy Concerns</i> ..... | 559 |
| 1. The FERC.....   | 559 |
| 2. The FCC .....   | 559 |

---

\* J.D., University of Colorado Law School (2011) and Associate Editor, University of Colorado Law Review. I am grateful for the helpful comments of Professor Paul Ohm, Professor Brad Bernthal, and the editorial board of the JTHTL, which benefited this Note. I would also like to thank Professor William Boyd, Eli Quinn, Mark Walker, and David Mohler for serving as soundboards in my search for the topic of this Note. Lastly, this Note is dedicated to Rich, Mary Ellen, Caitlin, and Seema. Without your support and encouragement over the past three years, this Note would not have been possible. Thank you.

3. The FTC, Its State Analogues, & PUCs ..... 560

IV. WHICH ENTITY SHOULD REGULATE NUSP-CONSUMER INTERACTIONS?..... 562

    A. *The FERC Should Regulate NUSP-Consumer Cyber Security Concerns*..... 562

        1. PUC Regulation Is Not Ideal ..... 562

        2. DOE Regulation Is Not Ideal ..... 565

        3. FCC Regulation Is Not Ideal ..... 566

        4. DHS Regulation Is Not Ideal..... 566

        5. FERC Regulation Is Optimal ..... 567

    B. *The FERC Should Regulate NUSP-Consumer Privacy Concerns*..... 569

CONCLUSION..... 571

INTRODUCTION

Enormous commercial interest surrounds the idea of modernizing the U.S. electric grid<sup>1</sup> via modern digital technology, more commonly known as creating the “smart grid.”<sup>2</sup> This interest is evidenced by the staggering amount of capital that continues to flow toward this end. The smart grid market is estimated to grow from \$20 billion in 2009, to \$42 billion in 2014,<sup>3</sup> and possibly to \$100 billion by 2030.<sup>4</sup> Additionally, the federal government has declared the modernization of the grid to be a priority for the U.S.<sup>5</sup> and has allocated \$3.4 billion in grants to smart grid development projects.<sup>6</sup> This tremendous public and private investment in the smart grid has led to the development of many products and services that promise to transform and modernize the grid in myriad ways. However, these avenues of modernization significantly complicate the regulation of the electric grid by blurring jurisdictional boundaries that already lack clarity. As a result, regulators are less able to quickly and adequately address issues that arise with smart grid development. This

---

1. Referred to interchangeably in this Note as “electric grid” or “grid.”

2. This paper will refer to modernization of the electrical grid as “smart grid development.” See generally LITOS STRATEGIC COMM’N, U.S. DEP’T OF ENERGY, THE SMART GRID: AN INTRODUCTION 2 (2008).

3. *U.S. Hardware and Software Companies Should Prepare to Capitalize on the Smart Grid in the U.S. and in International Markets*, ZPRYME RES. & CONSULTING (Dec. 2009).

4. *Wiser Wires*, ECONOMIST, Oct. 10, 2009, at 71 (citing a prediction by Morgan Stanley); see also ELEC. POWER RESEARCH INST., POWER DELIVERY SYSTEM OF THE FUTURE: A PRELIMINARY ESTIMATE OF COSTS AND BENEFITS 5-1 (2004) (stating that investment in the smart grid is likely to reach \$165 billion by 2024).

5. Energy Independence and Security Act of 2007 § 1301, 42 U.S.C.A. § 17831 (2010).

6. These funds were made available by the American Reinvestment and Recovery Act of 2009. *Smart Grid Investment Grant Awards*, DEP’T OF ENERGY, <http://www.oe.energy.gov/recovery/1249.htm> (last visited Feb. 11, 2011).

Note analyzes one such issue: the lack of clear jurisdictional authority to regulate the direct interactions between consumers and non-utility companies that offer smart grid products and services (“non-utility service providers” or “NUSPs”). This lack of regulatory authority is significant because inadequate oversight of these interactions raises substantial security and privacy concerns. Accordingly, this Note analyzes this issue in Part I by giving a brief overview of what smart grid development entails. Part II explains the security and privacy concerns of NUSPs developing the smart grid by interacting directly with consumers, and determines that these concerns are substantial enough to require regulation. Part III explores which entities have authority to regulate these interactions and determines that none do. Lastly, Part IV analyzes which entity should be given authority to regulate NUSP-consumer interactions, and concludes that the most appropriate solution is to extend the Federal Energy Regulatory Commission’s (“FERC”) current jurisdictional authority.

## I. OVERVIEW OF SMART GRID DEVELOPMENT

As stated above, the idea of modernizing the U.S. electric grid via modern digital technology is referred to as creating the “smart grid” or “smart grid development.”<sup>7</sup> Although there are wide differences between the seemingly endless number of new and developing smart grid products and services that purport to further this end, each generally involves the application of digital technology to the grid to enable real-time coordination of electric data.<sup>8,9</sup> Additionally, these products and services commonly seek to accomplish one or more recognized goals of smart grid development. These goals were laid out by the Energy Independence and Security Act of 2007 (“EISA”) and include: (1) the use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid, (2) integration of distributed resources and electric generation, including renewable resources, (3) deployment of “smart” digital technologies that optimize the operation of appliances and consumer devices through real-time monitoring, automation, and

---

7. *See supra* notes 1-2.

8. *Smart Grid*, FED. ENERGY REG. COMM’N, <http://www.ferc.gov/industries/electric/indus-act/smart-grid.asp> (last updated Feb. 2, 2011); *see also* DON VON DOLLEN, ELEC. POWER RESEARCH INST., REPORT TO NIST ON THE SMART GRID INTEROPERABILITY STANDARDS ROADMAP 6 (2009) (defining the smart grid as the “two-way flow of electricity and information to create an automated, widely distributed energy delivery network”).

9. It is very difficult to speak about smart grid technologies as a group because there is such a wide range of services, products, and business models currently in use or in development. Invariably some technology falls outside a given generalization. However, this fact should not reduce the value of this Note’s findings in relation to those technologies that it does encompass.

user interaction capabilities, and (4) provision of timely electric information and control options to consumers.<sup>10</sup> While these goals add some commonality between different smart grid products and services, the development of an advanced metering infrastructure (“AMI”) is considered the keystone to achieving the goals of the smart grid.<sup>11</sup>

AMI is a metering system that almost exclusively uses digital technology to record “customer consumption (and possibly other parameters) hourly or more frequently and provides for daily or more frequent transmittal of measurements over a communication network to a central collection point.”<sup>12</sup> Like most methods of modernizing the grid, AMI has many applications. However, two applications have emerged as the predominant foci: first, using advanced metering devices at the distribution level to create better communication between electric utilities and (usually) residential consumers, and second, supplying advanced metering products and services directly to consumers by NUSPs.<sup>13</sup> While both utility and non-utility products and services will likely have a role in the development of the smart grid, non-utility services may create some particularly difficult regulatory issues. Because it is unclear that any entity can effectively and comprehensively regulate interactions between consumers and NUSPs, leading to security and privacy concerns, this second category is the focus of this Note.<sup>14</sup>

## II. WHY NUSP-CONSUMER INTERACTIONS SHOULD BE REGULATED

Commentators note that there are many cyber security and privacy concerns related to the development of the smart grid.<sup>15</sup> These concerns

10. Energy Independence and Security Act of 2007 § 1305, 42 U.S.C.A. § 17385 (2010).

11. See LITOS STRATEGIC COMM’N, *supra* note 2, at 11 (describing two-way digital communication as a key function of the smart grid, which is made possible by AMI’s ability to allow electricity price-signals to reach consumers); OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEPT’ OF ENERGY, ADVANCED METERING INFRASTRUCTURE 2 (2008).

12. FED. ENERGY REGULATORY COMM’N, ASSESSMENT OF DEMAND RESPONSE AND ADVANCED METERING vi n.2 (2008).

13. See, e.g., *What Is TED?*, ENERGY, INC., <http://www.theenergydetective.com/what/overview.html> (last visited Feb. 11, 2011); *Products, ALERTME*, <http://www.alertme.com/products> (last visited Feb. 11, 2011).

14. See *infra* Part II.

15. See, e.g., SMART GRID INTEROPERABILITY PANEL – CYBER SEC. WORKING GRP., NAT’L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS 8, 111-12 (2010) [hereinafter NISTIR DRAFT FEB. 2010]; see also Investigation of Sec. & Privacy Concerns Regarding the Deployment of Smart Grid Tech., *Order Opening Docket, Establishing Procedures & Dates, & Seeking Comments & Information*, Colo. PUC Dkt. No. 09I-593EG, 2009 WL 2751604, at 2 ¶ 5 (Aug. 12, 2009) [hereinafter Investigation]; Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies* 9-11 (Working Paper Series, 2009).

have largely been evaluated with the presumption that smart grid development would be subject to regulation. However, it is not clear that this is true regarding NUSP-consumer interactions, potentially making these concerns more significant. This Part illustrates the magnitude of the risk associated with inadequate regulation of NUSP-consumer interactions by providing background information on NUSPs and the cyber security and privacy concerns created by their interactions with consumers. Section A explains what NUSPs are and how they provide smart grid products and services directly to consumers. Then, Section B describes the cyber security and personal privacy concerns that emerge when NUSPs provide smart grid products and services to consumers.<sup>16</sup>

### *A. What are NUSPs and How Do They Interact with Consumers?*

NUSPs interact directly with consumers by bypassing a consumer's electric utility and providing smart grid products and services ("non-utility services") directly to the consumers. NUSPs are able to avoid the involvement of the consumer's utility by relying on the consumer to provide electric usage data that the NUSP otherwise would need to obtain from the consumer's electric utility.<sup>17</sup> The two main examples of non-utility services are electric efficiency analysis ("EEA") and energy management, both of which are discussed below. These services are provided by NUSPs to consumers via many interfaces including advanced metering devices, Web portals, software, and home area networks ("HANs").<sup>18,19</sup>

EEA is a non-utility service that provides consumers with an analysis of their electricity usage, and in turn allows consumers to identify and eliminate energy sinks.<sup>20</sup> In effect, EEA provides consumers with the information necessary to correct electrical inefficiencies and

---

16. While this Note explains the privacy concerns related to NUSPs and details the regulatory framework surrounding them, it does not delve into the issue of how privacy concerns should be treated by NUSPs and regulators.

17. Some NUSPs collect electric usage data from electric utilities. However, this Note focuses on NUSPs that collect electric usage data directly from consumers because these services are less likely to fall under state PUC jurisdiction as they are farthest removed from the electric utility.

18. HANs are defined as the "network[s] between the advanced meter and the home device[s]" within an advanced metering system, which includes advanced meters, the associated hardware, and software and communications systems. PUB. UTIL. COMM'N OF TEX., GLOSSARY 2 (2009).

19. For more information about other non-utility services, see Quinn, *supra* note 15, at B-6 to -8 (noting that other uses of electric usage data include insurance premium calculation, marketing research, and national security and law enforcement).

20. Energy sinks are defined as "anything that collects a significant quantity of energy that is either lost or not considered transferable in the system under study." *Flow of Energy*, CONNEXIONS, <http://cnx.org/content/m16468/1.3> (last modified Sept. 25, 2009).

lower electric bills. Two examples of EEA are Google's PowerMeter<sup>21</sup> and Microsoft's Hohm, which both provide EEA through a Web portal interface using online software.<sup>22</sup> PowerMeter enables consumers to monitor their electricity usage<sup>23</sup> by allowing them "to view their home's energy consumption from anywhere online."<sup>24</sup> To monitor electricity usage, the software must receive electric usage data from the consumer's home. This could be accomplished by receiving data from a smart meter installed by a consumer's electric utility. However, PowerMeter bypasses the utility by receiving data directly from the consumer. This is done by providing the consumer with a device to install in his or her home that can collect data.<sup>25</sup> Alternatively, EEA can be performed without installing any sort of advanced meter. Microsoft's Hohm accomplishes this by requiring a consumer to manually enter certain energy-related information onto an online software program, which in turn provides efficiency suggestions<sup>26</sup> based on the consumer's "specific household circumstances including home attributes and use of appliances and systems."<sup>27</sup>

The other main non-utility service, energy management, usually includes EEA as part of the service, but takes EEA a step further by also providing a management system for a consumer to control electric usage throughout the residence.<sup>28</sup> Two examples of energy management, among others,<sup>29</sup> are AlertMe.com, Ltd.'s AlertMe Energy ("AlertMe")

21. *Google PowerMeter*, GOOGLE, <http://www.google.org/powermeter> (last visited Feb. 11, 2011).

22. *Help*, MICROSOFT HOHM, <http://www.microsoft-hohm.com/Info/Help.aspx> (under "Frequently Asked Questions" select "What is Hohm?") (last visited Feb. 11, 2011).

23. *See Google PowerMeter*, *supra* note 21. Other notable Web-based load management products/services are Silver Spring Network's Greenbox, *see Products*, SILVER SPRING NETWORKS, <http://silverspringnetworks.com/products/index.html> (last visited Feb. 11, 2011), and Agilewaves' Resource Monitor, *see Products*, AGILEWAVES, <http://www.agilewaves.com/products> (last visited Feb. 11, 2011).

24. *Google PowerMeter Frequently Asked Questions*, GOOGLE, <http://www.google.org/powermeter/faqs.html> (last visited Feb. 11, 2011).

25. *See infra* text accompanying notes 33-34; *see also supra* note 13.

26. Software load management serves the same purpose as Web portal load management services except that the software is not located online. Notable companies providing this type of load management include IBM and Cisco Systems who have combined their Tivoli software and EnergyWise company-wide energy management services, respectively. *EnergyWise Technology*, CISCO, [http://www.cisco.com/en/US/solutions/ns726/intro\\_content\\_energywise.html](http://www.cisco.com/en/US/solutions/ns726/intro_content_energywise.html) (last visited Feb. 11, 2011).

27. *Help*, *supra* note 22.

28. "[E]nergy management is the process of monitoring, controlling, and conserving energy . . ." *The What, Why, and How of Energy Management*, BIZEE ENERGY LENS, <http://www.energylens.com/articles/energy-management> (last visited Feb. 11, 2011).

29. *See* Jeffrey Lee, *Real Time Feedback*, ECOHOME (Feb. 6, 2009), <http://www.ecohomemagazine.com/home-technology/real-time-feedback.aspx> (noting Blueline Innovations' PowerCost Monitor and Control4's home controller as other non-utility

and Energy, Inc.'s The Energy Detective ("T.E.D.").<sup>30</sup> Both AlertMe and T.E.D. provide EEA to consumers through the installation of an advanced metering device in a consumer's home, which collects electricity usage data for the residence.<sup>31</sup> After collecting this data, AlertMe, and to a lesser extent T.E.D., helps consumers improve electric efficiency by allowing them to better control energy use in their home.<sup>32</sup> Installation of T.E.D. requires connecting hardware to the residence's circuit breakers and then plugging an LCD display into an electric socket.<sup>33</sup> AlertMe operates differently, requiring attachment of hardware onto the actual electric meter and setting up a broadband hub that collects usage data and transmits it over the Internet.<sup>34</sup> Both of these products bypass the electric utility. Additionally, both companies supplying these products have joined in a partnership with Google,<sup>35</sup> whereby their devices provide consumers with energy management service and Google's PowerMeter provides the EEA.<sup>36</sup>

Lastly, energy management is also provided by a broad category of products referred to as HANs. HANs are networks that come in many forms; one formal definition describes them as the "network[s] between the advanced meter and the home device[s]" within an advanced metering system, which includes advanced meters, the associated hardware, and software and communications systems.<sup>37</sup> HANs are essentially networks within a consumer's home that connect home appliances with heating, cooling, and lighting systems via an interface such as a website, software, or hardware.<sup>38</sup> Through this portal,

energy management service providers); *see also* Katie Fehrenbacher, *How Apple Could Jolt the Smart Home Energy Market*, GIGAOM (Jan. 17, 2010, 5:19 PM), <http://earth2tech.com/2010/01/17/how-apple-could-jolt-the-smart-home-energy-market>; Katie Fehrenbacher, *Intel Developing Home Energy Management Concept Gadget*, GigaOM (Sept. 24, 2009, 1:01 PM), <http://earth2tech.com/2009/09/24/intel-developing-home-energy-management-concept-gadget>.

30. *See What Is TED?*, *supra* note 13.

31. *How It Works*, ALERTME, <http://www.alertme.com/products/energy/how-it-works> (last visited Feb. 11, 2011); *What Is Ted?*, *supra* note 13.

32. *Id.*

33. *How Do I Install TED?*, THE ENERGY DETECTIVE, <http://www.theenergydetective.com/what/install.html> (last visited Feb. 11, 2011).

34. *Getting Started*, ALERTME, <http://www.alertme.com/help/getting-started> (last visited Feb. 11, 2011).

35. Katie Fehrenbacher, *Google's PowerMeter Links with AlertMe, UK Utility*, GIGAOM (Oct. 28, 2009, 7:29 AM), <http://earth2tech.com/2009/10/28/googles-powermeter-links-with-alertme-uk-utility>.

36. Katie Fehrenbacher, *How Google's PowerMeter Will Affect the Smart Grid Industry*, GIGAOM (Feb. 11, 2009, 12:00 AM), <http://earth2tech.com/2009/02/11/how-googles-powermeter-will-affect-the-smart-meter-industry>.

37. PUB. UTIL. COMM'N OF TEX., GLOSSARY, *supra* note 18.

38. *Home Area Networks*, BURNS & MCDONNELL, [http://www.burnsmcd.com/portal/page/portal/Internet/Service/Electrical\\_Transmission\\_and\\_Distribution1/SmartGrid/Home%20Area%20Network](http://www.burnsmcd.com/portal/page/portal/Internet/Service/Electrical_Transmission_and_Distribution1/SmartGrid/Home%20Area%20Network) (last visited Feb. 11, 2011).

consumers can obtain real-time information about the total energy use of their home and can make changes to this use in various ways.<sup>39</sup> Examples include automating energy use so that energy will only be used during periods of the day with the lowest prices, and programming appliances, heating, cooling, and distributed generation systems (e.g. solar panel displays) to operate as efficiently as possible.<sup>40</sup> HANs, like other energy management services, rely on obtaining electric usage data from some sort of advanced meter (utility or non-utility installed).<sup>41</sup> Although this meter can be installed by a utility or a NUSP, only HANs that utilize electric usage data gathered from the consumer without involving the consumer's electric utility are relevant to this Note.

### B. *Cyber Security and Privacy Concerns of NUSP-Consumer Interactions*

While the smart grid promises to increase the efficiency and reliability of the electric grid, it may also increase cyber security concerns for the grid and privacy concerns for consumers.<sup>42</sup> This Section outlines the scope of each of these concerns and highlights how they may be exacerbated by NUSP-consumer interactions.

#### 1. Cyber Security Concerns

Understanding cyber security concerns requires a basic understanding of prevailing terminology. Cyberspace is defined as an "interdependent network of information technology infrastructures"<sup>43</sup> including "the Internet, telecommunications networks, computer systems, and embedded processors and controllers."<sup>44</sup> Broadly, cyber security is the protection of these infrastructures.<sup>45</sup> More formally, cyber security is "the protection required to ensure confidentiality, integrity, and availability of the electronic information communication system."<sup>46</sup>

39. *Id.*

40. Lynne Kiesling, *Intelligent End-Use Devices Make a Transactive Smart Grid Valuable (Part 3 of 5)*, KNOWLEDGE PROBLEM (Mar. 4, 2009, 7:41 PM), <http://knowledgeproblem.com/2009/03/04/intelligent-end-use-devices-make-a-transactive-smart-grid-valuable-part-3-of-5>.

41. *Smart Meters and Home Area Networks*, SAN DIEGO GAS & ELECTRIC, <http://www.sdge.com/smartmeter/homeAreaNetwork.shtml> (last visited Feb. 11, 2011).

42. *See generally* Investigation, *supra* note 15.

43. U.S. DEP'T OF HOMELAND SEC., *THE NATIONAL STRATEGY TO SECURE CYBERSPACE* iii (2003).

44. Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 125 (2009) (quoting DEP'T OF DEF., *DICTIONARY OF MILITARY AND ASSOCIATED TERMS* 141 (2001)). *See* DEP'T. OF DEF., *DICTIONARY OF MILITARY AND ASSOCIATED TERMS* 92 (2010).

45. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 9-10.

46. *Id.* at 10; *see also* BRUCE S. SCHAEFFER ET AL., *CYBER CRIME AND CYBER*

Recently, the National Institute of Science and Technology (“NIST”) has called for a more inclusive definition of cyber security in relation to the development of the smart grid.<sup>47</sup> The NIST proposes expanding the definition of cyber security in relation to the smart grid to include “both power and cyber system technologies and processes in [information technology] and power system operations and governance.”<sup>48</sup> The NIST’s desire to develop a more precise definition of cyber security is part of its development of cyber security standards for the smart grid.<sup>49</sup> These standards are recognized as critical to the protection of the U.S. economy, which depends on the proper functioning of the information technology (“IT”) infrastructure and power system.<sup>50</sup>

The federal government officially recognized the need for strong cyber security standards in 2003, when such standards were deemed necessary to eliminate the risk of “organized cyber attacks capable of causing debilitating disruption to our Nation’s critical infrastructures, economy, or national security.”<sup>51</sup> In turn, cyber security emerged as a concern with the development of the smart grid because the smart grid relies heavily on software and networks to achieve its goals, which, if not adequately protected, can provide cyber criminals with a way to attack the electric grid and impact its overall safety and reliability.<sup>52</sup> As one FERC commissioner stated, “[t]he significant benefits of Smart Grid technologies must be achieved without taking reliability and security risks that could be exploited to cause great harm to our Nation’s citizens and economy.”<sup>53</sup> Ironically, because the smart grid seeks to increase the efficiency of the electric grid through the use of modern technology (such

SECURITY: A WHITE PAPER FOR FRANCHISORS, LICENSORS, AND OTHERS 1 (2009) (citing another definition of cyber security as “the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional”).

47. See NISTIR DRAFT FEB. 2010, *supra* note 15, at 10.

48. *Id.*

49. See *id.* at 10, 12.

50. *Id.* at 8 (noting that the need to address cyber security vulnerabilities has been acknowledged by many federal government agencies).

51. See U.S. DEP’T OF HOMELAND SEC., *supra* note 43, at viii.

52. *Id.* at xiii, 6; see also NISTIR DRAFT FEB. 2010, *supra* note 15, at 8-9 (citing one of the EISA’s explicit statements of purpose to include “modernization of the Nation’s electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure” in relation to the development of the Smart Grid, and noting that “[t]he need to address potential vulnerabilities has been acknowledged across the federal government, including the [NIST], the [DHS], the [DOE], and the [FERC]”).

53. *Smart Grid Initiatives and Technologies: Hearing to Examine the Progress on Smart Grid Initiatives Authorized in the Energy Independence and Security Act of 2007, and Funded in the Stimulus Bill, and to Learn of Opportunities and Impediments to Timely Installation of Smart Grid Technologies Before the S. Comm. on Energy & Natural Res.*, 111th Cong. 7 (2009) (prepared statement of Suedeen G. Kelly, Comm’r, Federal Energy Regulatory Commission).

as software and networks), and because software and networks are by their very nature prone to cyber attacks, smart grid development may actually decrease the security of the electric grid. This underscores the importance of prudent smart grid development that understands and adapts to the challenges of cyber security.

The EISA delegated responsibility to the NIST to develop “interoperability and functionality” standards for the smart grid.<sup>54</sup> The NIST has interpreted this authority to include cyber security standards,<sup>55</sup> which the NIST is still developing.<sup>56</sup> These standards currently target the ways that smart grid development may create cyber security risks such as (1) by increasing the complexity of the grid thereby introducing vulnerabilities and increasing exposure to attacks and unintentional errors, (2) by increasingly interconnecting networks, (3) by increasing vulnerabilities to communication disruptions and introduction of malicious software that could result in denial of service or compromising the integrity of software and systems, (4) by increasing the number of entry points and paths for attackers, and (5) by increasing the potential for compromise of data confidentiality.<sup>57</sup> These vulnerabilities are also created by NUSP-consumer interactions.

NUSP-consumer interactions should be considered a cyber security risk equal to other smart grid applications because the non-utility services they provide share the same vulnerabilities as other aspects of smart grid development. Non-utility services exhibit all of the smart grid development vulnerabilities identified above as particularly problematic for assuring the safety of the grid. First, these interactions increase the complexity of the grid by adding an additional layer of functionality to the grid. For example, AlertMe adds a new layer of functionality to the grid by creating an interface where the consumer can tap into his or her electric usage data to perform EEA. This new function complicates the current status of the grid by adding a function currently absent (i.e. the grid currently lacks active participation of the consumer beyond consuming electricity). Second, these interactions increase the interconnection of networks. HANs are good examples of this as they create new networks within a consumer’s home to perform EEA, which is in turn connected to the Internet. Third, many of these services increase vulnerability to malicious software and the potential for service disruption because they allow consumers to utilize the Internet to

---

54. Energy Independence and Security Act of 2007 § 1305, 42 U.S.C.A. § 17385 (2010); see also NAT’L INST. OF STANDARDS & TECH., NIST FRAMEWORK AND ROADMAP FOR SMART GRID INTEROPERABILITY STANDARDS RELEASE 1.0 7 (2010) (interpreting the NIST’s EISA authority to include cyber security standards).

55. NAT’L INST. OF STANDARDS & TECH., *supra* note 54.

56. See NISTIR DRAFT FEB. 2010, *supra* note 15, at 1.

57. *Id.* at 8.

perform EEA, which creates an additional access point for malicious software to exploit. Fourth, these new access points also create additional entry points that potential attackers can exploit to harm the grid. Finally, non-utility services such as PowerMeter or AlertMe create a risk that data confidentiality will be compromised because an additional party, the non-utility, collects electric usage data from consumers.<sup>58</sup>

Exploitation of poor cyber security related to NUSP-consumer interactions could result in harm to the grid in a variety of ways. As the complexity of interconnection between smart grid technologies and the electric grid increases, a “chain of dependencies” is created that makes the grid more and more vulnerable to cyber attacks.<sup>59</sup> The Department of Energy (“DOE”) has explained that these vulnerabilities could be exploited to jeopardize the grid, stating that there is potential for “extreme damage from a cyber attack” on the U.S. electric grid that could result in “destruction of generators, power outages, and grid instability.”<sup>60</sup> One way this level of damage could be achieved is by disruption of IT equipment by EM Pulse, EMI, or Geomagnetically Induced Currents.<sup>61</sup> More specifically, the DOE cited a 2009 study of AMI devices and networks to exemplify how a NUSP-consumer interaction could result in such “extreme damage.”<sup>62</sup> This study found that when these wireless AMI devices/networks (such as wireless non-utility devices that provide EEA and HANs connected to them) are used by consumers outside of the control of an electric utility, the devices are highly vulnerable to cyber attacks.<sup>63</sup> The study found that if these devices were attacked, the grid would be jeopardized by a cyber attacker extracting data from the memory of a device and modifying the device’s memory to insert malicious software.<sup>64</sup> Once the device has been compromised, it can be used to attack other parts of the smart grid by communicating through a network, which can compromise control systems.<sup>65</sup>

---

58. See Quinn, *supra* note 15, at 9-11.

59. Alex Yu Zheng, *Smart Security for a Smart Grid: New Threats on the Horizon*, SMARTGRIDNEWS.COM (Sept. 28, 2009), [http://www.smartgridnews.com/artman/publish/Technologies\\_Security\\_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html](http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html).

60. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP’T OF ENERGY, STUDY OF SECURITY ATTRIBUTES OF SMART GRID SYSTEMS – CURRENT CYBER SECURITY ISSUES 2 (2009).

61. ANNABELLE LEE, NAT’L INST. OF STANDARDS & TECH., U.S. DEP’T OF COMMERCE, NIST AND THE SMART GRID 32 (2010).

62. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 60, at 12 (citing Travis Goodspeed et al., *Low-level Design Vulnerabilities in Wireless Control Systems Hardware* (2009)).

63. *Id.*

64. *Id.*

65. *Id.*

Employees of the FERC have also acknowledged the cyber security concerns that develop due to chains of dependencies between the grid and NUSP-consumer interactions.<sup>66</sup> Joseph McClelland, Director of the Office of Electric Reliability at the FERC, has specifically addressed the danger of non-utility services.<sup>67</sup> McClelland has stated that “a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.”<sup>68</sup> He believes that these access points allow cyber attackers to harm the grid by either manipulating the electric usage data collected by non-utility devices or by manipulating the control systems that manage electricity supply and usage.<sup>69</sup> Additionally, McClelland singles out automated load management, one of the main functions of non-utility services, as a particularly apt avenue for attacking the grid.<sup>70</sup> He explains that an attack on load management could be used to affect the smart grid’s AMI, which could result in disconnection of service to a large number of customers and subsequently harm the bulk power system.<sup>71</sup> Reestablishing service could be greatly delayed if a subsequent attack was carried out on the advanced meters themselves.<sup>72</sup> This loss of service can be extremely costly—an estimated \$164 billion per year—and should be avoided.<sup>73</sup>

As the DOE findings and McClelland’s statements illustrate, the electric grid is vulnerable to damaging cyber security attacks that originate from NUSP-consumer interactions. As explained below, no entity has authority to effectively regulate these interactions.<sup>74</sup> Thus, to avoid this potential harm, it is necessary to create regulatory authority

66. See *Securing the Modern Electric Grid from Physical and Cyber Attacks: Hearing Before the Subcomm. on Emerging Threats, Cybersecurity, & Sci. & Tech. of the H. Comm. on Homeland Sec.*, 111th Cong. 51-52 (2009) (statement of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission).

67. *Id.*

68. *Id.* at 52.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. CONSORTIUM FOR ELEC. INFRASTRUCTURE TO SUPPORT A DIGITAL SOC’Y, THE COST OF POWER DISTURBANCES TO INDUSTRIAL & DIGITAL ECONOMY COMPANIES ES-3 (2001).

74. See *infra* Part III; see also ANNABELLE LEE, NAT’L INST. OF STANDARDS & TECH., SMART GRID CYBER SECURITY STRATEGY AND REQUIREMENTS A-19 (2009) [hereinafter NISTIR DRAFT SEPT. 2009] (describing the cyber security objectives for these interactions, but not going into detail for how they will be applied); Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010) (Standards for Interoperability in Federal Jurisdiction: “At any time after the Institute’s work has led to sufficient consensus in the Commission’s judgment, the Commission shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.”).

over the cyber security concerns that arise from NUSP-consumer interactions.

## 2. Privacy Concerns

While smart grid development may bring many positive benefits due to an improved ability to receive and transmit electric usage information, increased transmission of such information about individual consumers creates privacy concerns.<sup>75</sup> Examples of such concerns include the use of electricity usage data to (1) expose consumer behavior patterns for commercial benefit (e.g. through sale to advertising companies), (2) identify and track consumers for law enforcement purposes,<sup>76</sup> and (3) monitor consumer activities in the home.<sup>77</sup> While each of these capabilities of the smart grid could be used for beneficial purposes, they could also be used for malicious ones. Additionally, although it can be argued that the magnitude of harm that can result from such privacy violations is likely less severe in economic terms than the harm that can result from cyber security breaches,<sup>78</sup> the potential harm an individual consumer could experience through privacy violations is varied and personal. Not only could consumers experience monetary harm or a violation of their legal rights, but they could also be physically harmed through criminal acts made possible by the smart grid's data surveillance capabilities.<sup>79</sup> Accordingly, regulators and commentators have voiced concern that something must be done to protect consumer privacy in the context of smart grid services and products.<sup>80</sup>

As early as 2000, the National Association of Regulatory Utility Commissioners ("NARUC"), which represents the Public Utility Commissions ("PUC") of all fifty states,<sup>81</sup> adopted a resolution "[u]rging the [a]doption of [g]eneral [p]rivacy [p]rinciples [f]or [s]tate [c]ommission [u]se in [c]onsidering the [p]rivacy implications of the [u]se of [u]tility [c]ustomer [i]nformation."<sup>82</sup> Although the NARUC

75. See NISTIR DRAFT SEPT. 2009, *supra* note 74, at 8 (stating that there are "many significant privacy concerns and issues" regarding smart grid development); see also Quinn, *supra* note 15, at 11; *The Smart Grid and Privacy*, ELEC. PRIVACY INFO. CTR., <http://epic.org/privacy/smartgrid/smartgrid.html> (last visited Feb. 11, 2011).

76. Quinn, *supra* note 15, at 11.

77. For more technical information regarding how smart metering accomplishes these feats, see Quinn, *supra* note 15, at A-1 to -9.

78. See *supra* note 60 and accompanying text.

79. Quinn, *supra* note 15, at 10 (describing the potential for burglary as a privacy concern created by the smart grid's ability to obtain detailed electric usage data which could be used to ascertain when consumers are away from their homes).

80. See *supra* note 15.

81. *About NARUC*, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, <http://www.naruc.org/about.cfm> (last visited Feb. 11, 2011).

82. NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, RESOLUTION URGING THE

identified the privacy issues associated with smart grid development nearly ten years ago, the NIST noted in 2010 that “in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid” and that a “lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed.”<sup>83</sup> Such statements affirm the need to protect against privacy concerns related to smart grid development and evidence the current lack of such protections.

Finally, while it is unclear that either the NARUC’s or the NIST’s statements contemplated the role of NUSPs in smart grid development, privacy concerns are not reduced in this context. Instead, privacy concerns may be exacerbated for NUSP-consumer interactions because it is less clear which government entity can regulate such interactions. This uncertainty stems from the legal distinction between a utility-consumer interaction and a NUSP-consumer interaction, the former clearly being under PUC jurisdiction while the latter is a more difficult inquiry.<sup>84</sup> Regardless of this regulatory uncertainty, because privacy concerns related to smart grid development have been identified by regulatory authorities as serious concerns that need to be addressed, regulation of the privacy concerns of NUSP-consumer interactions is also necessary.

### III. WHAT ENTITY HAS AUTHORITY TO REGULATE NUSP-CONSUMER INTERACTIONS?

Determining what government entity or entities have authority to regulate the smart grid is complicated. This Part identifies the government entities with regulatory authority over the development of the smart grid, explains the extent of each entity’s regulatory authority, and concludes that none of these entities have authority to adequately regulate the cyber security and privacy concerns of NUSP-consumer interactions. Section A explains why no government entity currently has the authority to adequately regulate NUSP-consumer *cyber security* concerns, and Section B explains why the state PUCs and the state analogues of the Federal Trade Commission (“FTC”) are the only entities with authority to regulate NUSP-consumer *privacy* concerns.

---

ADOPTION OF GENERAL PRIVACY PRINCIPLES FOR STATE COMM’N USE IN CONSIDERING THE PRIVACY IMPLICATIONS OF THE USE OF UTILITY CUSTOMER INFORMATION (2000).

83. NISTIR DRAFT SEPT. 2009, *supra* note 74, at 8.

84. *See infra* Part III.

*A. No Entity has Authority to Regulate NUSP-Consumer Cyber Security Concerns*

Authority to regulate the electric grid was traditionally divided between the FERC and PUCs. The FERC's jurisdiction, as codified in the Federal Power Act ("FPA"),<sup>85</sup> included authority to regulate wholesale sales<sup>86</sup> of electricity in interstate commerce and transmission of electricity in interstate commerce. The PUCs' jurisdiction included authority to regulate retail sales of electricity,<sup>87</sup> local distribution of electricity, and the siting of power plants and transmission lines.<sup>88</sup> Federal legislation has since altered this dual regulatory framework. Specifically, the Energy Policy Act of 2005 ("EPAct of 2005") and the EISA have increased the FERC's regulatory authority and have extended regulatory authority to additional entities such as the Department of Energy ("DOE"), the National Electric Reliability Corporation ("NERC"), the National Institute of Standards and Technology ("NIST"), and the Federal Communications Commission ("FCC") (referred to collectively as "non-traditional entities"). Additionally, the Department of Homeland Security ("DHS") has been delegated some jurisdiction over cyber security concerns. Delegation of regulatory authority to non-traditional entities has been problematic because it has blurred jurisdictional boundaries. Consequently, determining which entity has authority to regulate new developments in the electric industry, such as NUSP-consumer interactions, has become more difficult. This Section analyzes the jurisdictional boundaries of each entity in relation to NUSP-consumer cyber security concerns and concludes that it is unlikely that the FERC, PUCs, or non-traditional entities have authority to adequately regulate them.

1. The FERC—Partial and Inadequate Regulatory Authority

While the FERC's traditional and newly delegated regulatory powers give it a great deal of power to regulate the electric grid, these powers do not include the authority to adequately regulate the cyber security aspects of NUSP-consumer interactions. This Subsection outlines the development of the FERC's authority to regulate the electric grid and explains why its current jurisdiction is not broad enough to

---

85. Federal Power Act § 201, 16 U.S.C. § 824 (2006).

86. "Wholesale sales" are defined as one between two entities who are not the ultimate users of the electricity. FRED BOSSELMAN ET AL., ENERGY, ECONOMICS, AND THE ENVIRONMENT 590 (3d ed. 2010).

87. "Retail sales" are defined as sales directly to an end user. *Id.*

88. U.S. GEN. ACCOUNTING OFFICE, GAO-03-726R, ELECTRICITY MARKETS: FERC'S ROLE IN PROTECTING CONSUMERS 2 (2003).

allow for adequate regulation of the NUSP-consumer cyber security concerns.

Although the FERC's traditional authority to regulate the transmission and wholesale sales of electricity that occur in interstate commerce has expanded over the years, this authority does not allow for regulation of NUSP-consumer cyber security concerns. The FERC's authority to regulate the transmission and wholesale sales of electricity that occur in interstate commerce has expanded for two reasons: (1) growth in the amount of interstate wholesale sales and transmission of electricity, and (2) judicial recognition of the physical properties of electricity.<sup>89</sup> The first reason for expansion relates to the development of the electric grid. When the FPA was passed, the electric grid had few interstate transmission lines because electricity markets were local.<sup>90</sup> However, as electricity markets grew, interstate interconnection increased, thereby increasing the FERC's regulatory power.<sup>91</sup> The second reason for expansion relates to judicial recognition of the physical properties of electric transmission. Physical scientists have explained, and courts have accepted, that due to the physical properties of electricity, when electricity is transmitted intrastate it should be deemed to be traveling *interstate* if that state's grid connects to another state's grid.<sup>92</sup> Thus, nearly all transmission of electricity is now deemed to be transmission in interstate commerce.<sup>93</sup> Additionally, the FERC's

---

89. See *Fed. Power Comm'n v. Fla. Power & Light Co.*, 404 U.S. 453, 463 (1972) (upholding the FERC's interpretation that its jurisdiction over wholesale sales in interstate commerce includes sales of electricity for resale when that electricity is transmitted via transmission lines that eventually connect to transmission lines of another state due to the physical properties of electricity transmission); see generally Brief for Electrical Engineers, Energy Economists and Physicists as Amici Curiae Supporting Respondents, *New York v. FERC*, 535 U.S. 1 (2002) (No. 00-568), (2001 WL 605124) (explaining that due to the physical properties of electricity, electricity flows at a tremendous pace on the wires of an interconnected grid and is not confined to the artificial boundaries of a state, but instead should be considered to be present at all locations where transmission lines run).

90. *National Electricity Policy: Federal Government Perspectives: Hearing Before the Subcomm. on Energy & Air Quality of the H. Comm. on Energy & Commerce*, 107th Cong. 34 (2001) (prepared statement of Hon. Francis Blake, Deputy Secretary, Dep't of Energy).

91. See *supra* note 89. See also Jared M. Fleisher, ERCOT'S JURISDICTIONAL STATUS: A LEGAL HISTORY AND CONTEMPORARY APPRAISAL, 3 *TEX. J. OIL, GAS, & ENERGY L.* 4, 9-10 (2008) (describing the Supreme Court's "technological transmission test" for determining when electric transmission occurs in interstate commerce as laid out by *Conn. Light & Power Co. v. Fed. Power Comm'n*, 324 U.S. 515, 529-31 (1954), and how the test has been applied expansively).

92. See Fleisher, *supra* note 91, at 9 (describing how Texas, Alaska, and Hawaii are the only states that currently are not regulated by the FERC due to the broad interpretation of electric "transmission in interstate commerce").

93. See *Securing the Modern Electric Grid from Physical and Cyber Attacks*, *supra* note 66. It is also noteworthy that this recognition by the courts was the reason that Texas limited the connection of its transmission lines to those of surrounding states. Thus, Texas has escaped some regulation by the FERC and instead regulates the transmission of electricity within its

authority to regulate wholesale sales of electricity in interstate commerce has grown in proportion to this new interpretation of interstate transmission because wholesale sales are now much more frequently found to be in interstate commerce.<sup>94</sup>

Regardless of the expansion of the FERC's traditional regulatory powers, the FERC does not have authority to regulate NUSP-consumer interactions because these interactions do not involve either the wholesale sale or transmission of electricity. Wholesale sales of electricity are sales of electricity between entities who are not the ultimate users of the electricity.<sup>95</sup> Transmission of electricity is the physical transport or flow of electric energy to end use locations.<sup>96</sup> NUSP-consumer interactions involve the provision of a product or service by NUSPs to consumers that can be used for EEA or load management.<sup>97</sup> These services are performed by gathering a consumer's electric usage data and then analyzing it so that the consumer can make decisions about electricity use.<sup>98</sup> Because NUSP products/services allow consumers to collect and analyze electric usage data, but do not transmit or sell electricity to the consumer, NUSP-consumer interactions do not involve wholesale sale or transmission of electricity, and the FERC cannot regulate them under its traditional regulatory authority. Thus, the FERC must seek another jurisdictional hook if it is to regulate NUSP-consumer interactions.

Fortunately for the FERC, Congress has increased the FERC's range of jurisdictional powers via three major statutes: the EPAct of 2005,<sup>99</sup> the EISA,<sup>100</sup> and the ARRA.<sup>101</sup> Each of these statutes extends partial regulatory authority to the FERC for NUSP-consumer interactions. However, this partial authority is inadequate to properly address NUSP-consumer cyber security concerns.

The EPAct of 2005 changed the traditional electric regulatory framework by giving the FERC authority to regulate the "reliability" of

state via its own Electric Reliability Council of Texas (ERCOT). See *ERCOT*, FED. ENERGY REGULATORY COMM'N, <http://www.ferc.gov/industries/electric/indus-act/rto/ercot.asp> (last updated Jan. 20, 2011).

94. See *Fed. Power Comm'n v. Fla. Power & Light Co.*, 404 U.S. 453 (1972).

95. See FRED BOSSELMAN ET AL., *supra* note 86.

96. *Electric Power Transmission*, ANSWERS.COM, <http://www.answers.com/topic/electric-power-transmission> (last visited Feb. 11, 2011) (providing the definition from the McGraw-Hill Dictionary of Scientific and Technical Terms (6th ed. 2003)); see also Fleisher, *supra* note 91, at 9.

97. See *supra* Part II.A.

98. *Id.*

99. Codified as an amendment to the Federal Power Act at 16 U.S.C. § 824 (2006).

100. Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010).

101. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (to be codified in scattered sections of 42 U.S.C.).

the “bulk power system.”<sup>102</sup> To accomplish this, the FERC was ordered to appoint an electric reliability organization (“ERO”) that would establish mandatory electric reliability standards.<sup>103</sup> The FERC could then adopt and enforce these electric reliability standards via civil penalties.<sup>104</sup> In 2006, the FERC approved the North American Electric Reliability Corporation (“NERC”) to become the ERO, and in 2007 the FERC approved mandatory reliability standards suggested by the NERC.<sup>105</sup> The FERC’s authority to regulate the reliability of the grid arguably encompasses the regulation of cyber security concerns related to smart grid development because security violations have the potential to jeopardize the reliability of the grid.<sup>106</sup> However, at best this authority would only be a partial solution to these concerns because its powers would only extend to the “reliability” of smart grid development within the “bulk power system.”<sup>107</sup>

Reliability or “reliable operation” as codified in § 215(a)(4) of the FPA is defined as

[O]perating the elements of the Bulk-Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a Cybersecurity Incident, or unanticipated failure of system elements.<sup>108</sup>

This definition clearly contemplates cyber security as a component of “reliable operation.” However, the ability to use this provision to regulate the cyber security concerns of smart grid development is extinguished by the limitation that the FERC may only regulate cyber security when it involves the reliable operation of the “bulk power system.”

The “bulk power system” is defined as both “facilities and control systems necessary for operating an interconnected electric energy transmission network” and “electric energy from generating facilities needed to maintain transmission system reliability.”<sup>109</sup> The EPAct of 2005 specifically excludes “facilities used in the local distribution of

102. 16 U.S.C. § 824(o)(b)(1) (2006).

103. *Id.* §§ 824(o)(d-e).

104. *Id.*

105. N. AM. ELEC. RELIABILITY CORP., MILESTONES: NERC RELIABILITY STANDARDS 4 (2007).

106. This argument is based on an assumption that the cyber security threats are a consideration for the grid’s “reliability.”

107. 16 U.S.C. § 824(o)(a)(1) (2006).

108. 18 C.F.R. § 39.1 (2010).

109. *Id.*

electric energy”<sup>110</sup> from this definition. However, it is unclear what is considered a local distribution facility and what is considered part of the bulk power system.<sup>111</sup> Some employees at the FERC have stated that the bulk power system definition excludes nearly all grid facilities in some large cities,<sup>112</sup> while others state that it describes “low-voltage facilities used to deliver energy in one direction to retail end-users.”<sup>113</sup> Because general development of the smart grid, such as the provision of smart meters, largely takes place at the local distribution facilities and grid facilities,<sup>114</sup> this development falls outside of the FERC’s reliability authority. This is unfortunate because smart meters might be considered “control systems” under the definition of bulk power system. Control systems are defined as “facilities, systems, equipment, services, and diagnostics that provide the functional control capabilities necessary for the effective and reliable operation of the bulk [power] system.”<sup>115</sup> Smart meters perform this exact role by providing functional control of electric usage for effective operation of the grid. However, because the EPAct of 2005 specifically excludes local distribution and grid facilities, where smart meters are primarily located, smart meters are likely excluded from the bulk power system definition. Thus, it is likely that the FERC’s regulatory authority over grid reliability does not extend to the cyber security concerns of smart grid development taking place at local distribution and grid facilities.

The FERC’s reliability authority is even less likely to cover NUSP-consumer interactions. These interactions are presumably outside the scope of the bulk power system definition because these interactions are not similar to large scale control systems. The definition of bulk power system seems to contemplate large scale grid operations such as “facilities and control systems” used for operating a transmission network. NUSP-consumer interactions do not occur on a large scale, but instead are more localized and thus farther removed from the bulk power system than local distribution or grid facilities, which are exempted from the bulk power system definition. In fact, NUSP-consumer interactions take place at the smallest and most local level possible: the consumer’s residence. Additionally, it is unclear that NUSP services are control systems used for “operating a transmission network.” NERC’s reliability standards

---

110. 16 U.S.C. § 824(o)(a)(1) (2006).

111. BERNARD C. LESIEUTRE ET. AL., TOPOLOGICAL AND IMPEDANCE ELEMENT RANKING (TIER) OF THE BULK-POWER SYSTEM, PRELIMINARY REPORT 7 (2009).

112. See *Securing the Modern Electric Grid from Physical and Cyber Attacks*, *supra* note 66.

113. *Net Metering: Hearing Before the Subcomm. on Energy of the S. Comm. on Energy & Natural Res.*, 111th Cong. 5 (2009) (statement of Kevin A. Kelly, Director, Div. of Policy Dev., Office of Energy Policy and Innovation, Fed. Energy Regulatory Comm’n).

114. See generally U.S. DEPT OF ENERGY, *supra* note 2, at 2.

115. U.S. DEPT OF ENERGY & U.S. DEPT OF HOMELAND SEC., ROADMAP TO SECURE CONTROL SYSTEMS IN THE ENERGY SECTOR 5 (2006).

describe one such control system as “[s]ystems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.”<sup>116</sup> NUSP services, however, are used by the consumer in monitoring and augmenting electricity usage—a function that has nothing to do with transmission and which controls electricity usage many magnitudes of scale smaller than 300 MW.<sup>117</sup> Thus, it is likely that the FERC cannot regulate NUSP-consumer interactions to account for cyber security concerns or other larger scale aspects of smart grid development through its EPCRA of 2005 reliability authority because these interactions do not meet the definitional criteria over which the FERC has reliability authority.

Although the EPCRA of 2005 fails to vest the FERC with the jurisdiction needed to adequately regulate the cyber security concerns of smart grid development and NUSPs, the EISA does provide it with new jurisdiction tied directly to smart grid development.<sup>118</sup> This jurisdiction gives the FERC the power to regulate NUSP-consumer interactions, but because the FERC has interpreted its authority under this act narrowly,<sup>119</sup> the FERC cannot use its EISA authority to adequately address NUSP-consumer cyber security concerns without reinterpreting its jurisdictional authority.

The EISA has changed the traditional electric regulatory framework by directing the NIST to develop standards to ensure smart grid functionality and interoperability.<sup>120</sup> Interoperability is defined as “the capability of systems or units to provide and receive services and information between each other, and to use the services and information exchanged . . . without significant user intervention.”<sup>121</sup> Once the NIST has developed these standards, the FERC is required to institute rulemaking proceedings to adopt them, provided they “insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.”<sup>122</sup> The FERC has interpreted this delegation of authority to mean that it may adopt

116. N. AM. ELEC. RELIABILITY CORP., RELIABILITY STANDARDS FOR THE BULK ELECTRIC SYSTEMS OF NORTH AMERICA 2 in Standard CIP-002-1 (2006).

117. According to the U.S. Energy Information Administration, in 2008 the average U.S. household used only 11.04 MWh *per year* which equals 0.00126 MW needed each hour of every day (i.e., 11.04 MWh/y ÷ 365 days ÷ 24 hours/day). *Frequently Asked Questions – Electricity*, U.S. ENERGY INFO. ADMIN., [http://tonto.eia.doe.gov/ask/electricity\\_faqs.asp#electricity\\_use\\_home](http://tonto.eia.doe.gov/ask/electricity_faqs.asp#electricity_use_home) (last visited Feb. 11, 2011) (select “How much electricity does an American home use?”).

118. Smart Grid Policy, 74 Fed. Reg. 37,098, 37,098 (July 16, 2009).

119. *Id.* at 37,100.

120. *Id.* at 37,099.

121. GRIDWISE ARCHITECTURE COUNCIL, INTRODUCTION TO INTEROPERABILITY AND DECISION-MAKER'S INTEROPERABILITY CHECKLIST VERSION 1.5, 1 (2010).

122. Energy Independence and Security Act of 2007 § 1305(d), 42 U.S.C.A. § 17385(d) (2010).

interoperability standards for “all electric power facilities and devices with smart grid features, including those at the local distribution level and those used directly by retail customers so long as the standard is necessary for the purpose [stated in the act].”<sup>123</sup> Because NUSP devices, such as the TED or AlertMe, are “devices with smart grid features” and are used “directly by retail consumers,” the FERC has authority to regulate these devices through NIST standards as long as the standards are necessary for insuring “functionality and interoperability in interstate transmission of electric power, and . . . wholesale electricity markets.”<sup>124</sup> This power very nearly gives the FERC the ability to address the cyber security concerns of NUSPs. However, the FERC has interpreted a limitation on this new power that significantly restricts its efficacy: the EISA omits the additional authority for FERC to mandate or enforce these standards.<sup>125</sup> The FERC acknowledged this limitation in its Smart Grid Policy Statement by stating that it “does not [have] authority to . . . enforce [these] standards” or to “direct states to implement any particular retail customer policies or programs.”<sup>126</sup> Thus, while the FERC has the authority to enact standards that address NUSP-consumer cyber security concerns, the FERC effectively cannot ensure that these concerns are actually minimized. Accordingly, the only solutions available are for the FERC to reinterpret its interoperability authority or, as suggested by the FERC Commissioner Suedeen Kelly, for Congress to consider additional legislation.<sup>127</sup>

Although the FERC’s self-imposed enforcement limitation significantly restricts the efficacy of the interoperability standards, the FERC does have a limited ability to enforce the standards indirectly via its traditional cost-recovery ratemaking powers. Under this alternative, the FERC could bypass the limitation by mandating the adoption of the interoperability standards as a condition of parties recovering costs through rate regulation under the FERC’s traditional wholesale sales and transmission in interstate commerce jurisdiction.<sup>128</sup> The FERC has acknowledged its intention to do this in its Smart Grid Policy Statement,<sup>129</sup> explaining that while standards are being developed it will condition cost recovery on principles laid out in its “Interim Rate Policy.”<sup>130</sup> This policy requires applicants seeking smart grid cost recovery to (1) demonstrate that “the reliability and security of the bulk-power

---

123. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

124. 42 U.S.C.A. § 17385(d) (2010).

125. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 10.

126. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

127. *Id.*

128. *Id.* at 37,099.

129. *Id.* at 37,098.

130. *Id.* at 37,110.

system will not be adversely affected by the deployment of smart grid facilities at issue,<sup>131</sup> (2) show that it has minimized the possibility of stranded costs for smart grid equipment,<sup>132</sup> and (3) share certain information with the DOE Smart Grid Clearinghouse so that the smart grid deployment provides useful feedback for the development of the interoperability standards.<sup>133</sup> This indirect enforcement of the interoperability standards will allow the FERC to bypass its self-imposed jurisdictional limitation. However, it will not allow the FERC to regulate the cyber security concerns of smart grid development related to NUSP-consumer interactions because NUSPs are not utilities that will seek cost recovery, and even if they were, NUSP services would not fall under the FERC's ratemaking authority because they are not wholesale sales of electricity.<sup>134</sup> Thus, these interactions will go unregulated by the FERC.

## 2. PUCs—No Authority to Regulate

The powers of PUCs to regulate the electric grid are limited by the powers of the FERC, a state's constitution and legislation, and the U.S. Constitution.<sup>135</sup> Under this framework, the powers of PUCs may, at the maximum, extend to all the powers not delegated to the FERC and not precluded by the U.S. Constitution. In reality, PUC powers vary somewhat from state to state.<sup>136</sup> However, a PUC's electric regulatory authority generally includes the power to regulate the facilities, services, and rates of electric utilities operating within that state for the purposes of selling retail electricity and distributing electricity locally.<sup>137</sup> Under this general regulatory authority, a cursory analysis of NUSP-consumer interactions is enough to demonstrate that PUCs do not have the authority to regulate the NUSP-consumer cyber security concerns because NUSP-consumer interactions occur between non-utilities and consumers, and PUCs can only regulate interactions between utilities and consumers.

131. *Id.* at 37,111.

132. *Id.*

133. *Id.*

134. *See infra* Part III.A.2.

135. For example, the COLO. CONST., art. XXV, the COLO. REV. STAT. ANN. §§ 40-1-101 to -104 (West 2010), and the COLO. CODE REGS. § 723-1 (2011), lay out the powers of the Colorado PUC.

136. For example, California's PUC can regulate public utilities, including "electrical corporations," defined as any person or corporation owning, controlling, operating, or managing any electric plant for compensation within California "where the service is performed for, or the commodity is delivered to, the public or any portion thereof." CAL. PUB. UTIL. CODE § 216 (West 2010). Whereas in Texas the PUC can regulate public utilities including "electric utilities" defined as "a person . . . that owns or operates for compensation in [Texas] equipment or facilities to produce, generate, transmit, distribute, sell, or furnish electricity" in Texas. 16 TEX. ADMIN. CODE §§ 25.5(41), (92) (2011).

137. *See supra* text accompanying notes 87-88.

In relation to the new powers of the FERC and other new entities, PUCs retain a great deal of control over how the smart grid develops. As the FERC was careful to point out in its Smart Grid Policy Statement, PUCs retain authority to decide (1) what costs utilities may recover from ratepayers for smart grid development when that development relates to retail sales or local distribution of electricity, (2) whether or not to adopt interoperability and functionality standards for the smart grid, and (3) how to regulate retail electric consumers in relation to the smart grid.<sup>138</sup> These powers are strong tools for controlling smart grid development. For example, PUCs can choose to ignore the FERC's interoperability and functionality standards for smart grid devices/services and create their own when those devices/services are only used for the purposes of retail sales or local distribution of electricity.<sup>139</sup> Additionally, PUCs can control smart grid development by using their ratemaking authority to limit the types of smart grid expenditures which may be recovered through rate regulation. Lastly, and most importantly, a PUC can control the policies surrounding retail sales and local distribution of electricity, which encompasses the actual implementation and function of smart grid technologies. Through this power the PUC can determine how advanced meters are installed and how they allow consumers to respond to real-time pricing. Because many aspects of smart grid development depend upon PUC decisions in these three areas, PUCs retain substantial control over how the smart grid develops. However, this control does not extend to NUSP-consumer interactions.

PUCs regulate "public utilities." The definition of "public utility" is derived from English common law,<sup>140</sup> was formally adopted by the Supreme Court in *Munn v. Illinois*,<sup>141</sup> and has been codified in state statutes.<sup>142</sup> The common law defines a public utility as private property "affected with a public interest."<sup>143</sup> In turn, the common law considers private property to be affected with a public interest when it is "used in a manner to make it of public consequence, and affect the community at large."<sup>144</sup> In practice this definition seems difficult to apply. However, states have eliminated the need to use the definition on an ad hoc basis

---

138. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

139. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 10 (in which FERC Commissioner Suedeen Kelly states that even asserting the full scope of the FERC's powers under the FPA, the FERC's Smart Grid standards will only apply to certain entities, excluding PUCs).

140. *Munn v. Illinois*, 94 U.S. 113, 126 (1876) (citing Lord Chief Justice Hale's treatise, *DE PORTIBUS MARIS*, as the source of the definition of public utility).

141. *Id.*

142. See, e.g., COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010) (stating any entity "declared by law to be affected with a public interest" is a public utility).

143. *Munn*, 94 U.S. at 126.

144. *Id.*

by supplying concrete statutory lists of the entities that the state declares to be public utilities.<sup>145</sup> The entities declared to be public utilities in most states are those that “provide[] necessary services to the public, such as telephone lines and service, electricity, and water.”<sup>146</sup> Additionally, “[m]ost utilities operate as monopolies” that carry on operations “for the accommodation of the public, the members of which are entitled as a matter of right to use the enterprise’s facilities.”<sup>147</sup>

A sample of state definitions of public utility suggests that NUSPs are likely not public utilities. For example, in California public utilities include “electrical corporations” defined as any person or corporation owning, controlling, operating, or managing any electric plant for compensation within California “where the service is performed for, or the commodity is delivered to, the public or any portion thereof.”<sup>148</sup> Colorado’s definition of a public utility is nearly identical, stating that electrical corporations are deemed to be public utilities if they operate for the purpose of supplying the public with use of electricity.<sup>149</sup> Additionally, in Texas, public utilities include “electric utilities” defined as “a person . . . that owns or operates for compensation in [Texas] equipment or facilities to produce, generate, transmit, distribute, sell, or furnish electricity” in Texas.<sup>150</sup> A common thread among these states’ definitions is the limitation that for private corporations to be declared public utilities they must provide an electric service related to the *provision* of electricity to the consumer. This limitation guides the application of the definition and leaves out corporations such as NUSPs that provide services that are related to the *use* of electricity *by* the consumer. It also clearly leaves out NUSPs that provide products to consumers rather than services.

Even if one believes that it is ambiguous as to whether or not NUSPs fall under a state’s public utility definition, NUSPs are unlikely to be deemed public utilities by a state court because they do not meet the underlying limitation guiding decisions as to when a private enterprise should be deemed a public utility. For example, in applying the limitation outlined above to NUSPs such as Energy, Inc. or Alterm.com, Ltd., neither provides necessary services to the public similar to the provision of electricity or water, neither are monopolies,

---

145. Colorado defines a “public utility” as “every common carrier, pipeline corporation, gas corporation, electrical corporation, telephone corporation, water corporation, person, or municipality operating for the purpose of supplying the public for domestic, mechanical, or public uses and every corporation, or person declared by law to be affected with a public interest.” COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010).

146. BLACK’S LAW DICTIONARY 1686 (9th ed. 2009).

147. *Id.*

148. CAL. PUB. UTIL. CODE § 216 (West 2010).

149. *See* COLO. REV. STAT. § 40-1-103(1)(a)(I) (2010).

150. 16 TEX. ADMIN. CODE §§ 25.5(41), (92) (2011).

and members of the public are not entitled as a matter of right to use either companies' services. Instead, these companies conduct business as for-profit associations, the services they provide are simply beneficial to the consumer but not "necessary," and the members of the public only have a right to use these companies' services upon entering into private contracts with them. Thus, NUSPs are not public utilities, and NUSP-consumer interactions cannot be regulated by PUCs.

### 3. The DOE—No Authority to Regulate

The EISA charged the DOE with the responsibility of creating a Smart Grid Task Force ("SGTF") to "insure awareness, coordination and integration of . . . Federal Government [activities] related to smart-grid technologies and practices."<sup>151</sup> However, this grant of authority cannot be construed to grant the DOE power to regulate NUSP-consumer cyber security concerns.

The plain language of the EISA indicates that the DOE may create the SGTF for the limited purpose of streamlining federal government smart grid development efforts by allowing the SGTF to advise other agencies on the development of the smart grid.<sup>152</sup> Without more, the DOE cannot interpret this language to permit it to regulate NUSP-consumer interactions because such a delegation of authority is significant enough to necessitate plain statutory language.<sup>153</sup> Moreover, if the DOE attempted to take on this authority it is likely that the very purpose of the SGTF provision would be frustrated because it would inject confusion into the regulation and development of the smart grid by splitting up regulatory authority over the smart grid. Thus, the DOE does not have authority to regulate NUSP-consumer interactions via this provision.

The ARRA also charged the DOE with some responsibility over the development of the smart grid. The ARRA charged the DOE with the responsibility of awarding grants for smart grid projects and developing a smart grid information clearinghouse.<sup>154</sup> Responsibility for

---

151. Energy Independence and Security Act of 2007 § 1303(b)(2), 42 U.S.C.A. § 17383(b)(2) (2010).

152. *Id.* § 17383(a)(2) (stating the mission of the Smart Grid Advisory Committee, which oversees the SGTF, "shall be to advise the Secretary, the Assistant Secretary, and other relevant Federal officials concerning the development of smart grid technologies, the progress of a national transition to the use of smart-grid technologies and services, the evolution of widely-accepted technical and practical standards and protocols to allow interoperability and inter-communication among smart-grid capable devices, and the optimum means of using Federal incentive authority to encourage such progress").

153. *See generally* YULE KIM, CONG. RESEARCH SERV., STATUTORY INTERPRETATION: GENERAL PRINCIPLES AND RECENT TRENDS 39 (2008).

154. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 405, 123 Stat. 115 (to be codified at 42 U.S.C. § 17384).

developing a smart grid information clearinghouse does not permit the DOE to regulate the cyber security aspects of NUSP-consumer interactions. The DOE has interpreted this responsibility to mean that it must provide “comprehensive and detailed information about the attributes, performance, impacts, costs, and benefits of smart grid technologies, tools, and techniques” through “direct sharing and dissemination of information on knowledge gained, lessons learned, and best practices.”<sup>155</sup> Although authority to create the clearinghouse allows the DOE to create an information resource by requiring disclosure of information from smart grid grant applicants, it does not authorize the DOE to do more than collect data and even this power is restricted to entities that apply for a grant award.<sup>156</sup> Thus, this new responsibility does not extend to the DOE the power to regulate NUSP-consumer interactions.

Although the authority to award smart grid grants gave the DOE a small amount of control over NUSP-consumer interactions, the opportunity to exercise this power has passed because the DOE has already issued its grants.<sup>157</sup> The DOE had the responsibility to award smart grid grants, which it interpreted to mean authority to evaluate the cyber security vulnerabilities of proposed smart grid projects and reject those that “cannot provide reasonable assurance that their approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach.”<sup>158</sup> It also interpreted this responsibility to allow it to require a potential grant recipient to show that its project would use “open protocols and standards . . . if available and appropriate” to facilitate interoperability by allowing vendors to design and build smart grid equipment and systems that can function in tandem with the approved projects.<sup>159</sup> These interpretations of the DOE’s smart grid grant authority allowed the DOE to control the security issues of smart grid grants by rejecting projects that did not meet threshold security standards. However, the DOE has already exercised this grant authority so it cannot further control the security issues related

---

155. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, U.S. DEP’T OF ENERGY, RECOVERY ACT: FINANCIAL ASSISTANCE OPPORTUNITY FUNDING ANNOUNCEMENT 9 (2009), [available at http://www.bpa.gov/energy/n/smart\\_grid/docs/1306\\_Smart\\_Grid\\_investment\\_program\\_funding\\_announcement.doc](http://www.bpa.gov/energy/n/smart_grid/docs/1306_Smart_Grid_investment_program_funding_announcement.doc).

156. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 5-6.

157. *Will We Get Our Money’s Worth? \$3.4 Billion in Smart Grid Stimulus Grants Go to 100 Projects*, SMARTGRIDNEWS.COM (Oct. 27, 2009), [http://www.smartgridnews.com/artman/publish/Stimulus\\_News\\_Digest\\_News/Will-We-Get-Our-Money-s-Worth-3-4-Billion-in-Smart-Grid-Stimulus-Grants-Go-to-100-Projects-1336.html](http://www.smartgridnews.com/artman/publish/Stimulus_News_Digest_News/Will-We-Get-Our-Money-s-Worth-3-4-Billion-in-Smart-Grid-Stimulus-Grants-Go-to-100-Projects-1336.html).

158. OFFICE OF ELEC. DELIVERY & ENERGY RELIABILITY, *supra* note 155, at 40.

159. Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,113 n.179 (July 16, 2009).

to NUSP-consumer interactions. Thus, unless additional funding is allocated to the DOE under the same authority, the DOE no longer has the ability to regulate NUSP-consumer cyber security concerns via the smart grid grant authority.

#### 4. The FCC—Perhaps Able But Unlikely to Regulate

The ARRA directed the FCC to develop a National Broadband Plan (“NBP”) which includes “a plan for use of broadband infrastructure and services in advancing . . . energy independence and efficiency.”<sup>160</sup> In turn, the FCC, believing that its role should be to update policies, set standards, and align incentives to maximize broadband use for national priorities, has interpreted this authority to include development of an NBP that takes into consideration the energy sector, smart grid development, and cyber security.<sup>161</sup> Consequently, the FCC has made recommendations in the NBP that seek to modernize the electric grid with broadband so that it is more reliable and efficient and will allow for energy innovation in homes and buildings by making electric usage data readily accessible to consumers.<sup>162</sup>

Although it is difficult to see how the FCC’s new authority and agenda fit into the mix of agencies with partial authority over smart grid development, the FCC has interpreted its role to be one of guidance and assistance rather than active involvement. This is evidenced by the FCC’s decision to limit its ARRA authority to the narrow meaning of “plan” within its mandate of developing a “plan for use of broadband . . . in advancing . . . energy independence and efficiency.”<sup>163</sup> In other words, instead of developing a “plan” that involves active involvement by the FCC, the agency has limited the plan’s scope to offering recommendations to the principal agencies, states, and stakeholders that are currently participating in smart grid development.<sup>164</sup> Accordingly, while it is possible for the FCC to adopt a more aggressive interpretation of its role in smart grid development via its ARRA mandate, for the time being it seems likely that the FCC will only have a voice in developing cyber security standards for the smart grid and perhaps NUSPs. Moreover, the FCC may be hesitant to define its role as one of active

---

160. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001(k)(2)(D), 123 Stat. 115 (to be codified at 47 U.S.C. § 1305); *see also* Fed. Comm’n Comm’n, Comment Sought on the Implementation of Smart Grid Technology, GN Dkt. Nos. 09-47, 09-51, 09-137, NBP Public Notice #2 (2009), *available at* [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DA-09-2017A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2017A1.pdf).

161. FED. COMM’NS COMM’N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 7-11 (2010).

162. *Id.* at xiv.

163. American Recovery and Reinvestment Act of 2009 § 6001(k)(2)(D).

164. *Id.* § 6001(k).

regulation because such a decision would significantly complicate the regulatory landscape by adding another agency to the administrative process. Thus, although the FCC might have regulatory authority to address NUSP-consumer cyber security concerns, it seems unlikely that it will claim this authority.

## 5. The DHS—No Authority to Regulate

The DHS has some responsibility for addressing the nation's cyber security concerns. However, this responsibility does not extend to the regulation of NUSP-consumer interactions.

The DHS was given responsibility for the cyber security of non-federal entities in the Homeland Security Act of 2002.<sup>165</sup> However, this responsibility was limited to the provision of analysis, warnings, and crisis management support related to threats to, and vulnerabilities of, critical information systems as well as technical assistance (upon request) for “emergency recovery plans for failures of critical information systems.”<sup>166</sup> In other words, the DHS has no authority to mandate these standards, but can only suggest them, offer help in implementing them if requested, or help private parties create plans to address cyber security concerns.<sup>167</sup> For instance, the DHS worked with the DOE to create the “Roadmap to Secure Control Systems in the Energy Sector” in 2006.<sup>168</sup> This document outlines a vision of both departments and stakeholders of the electric energy industry in which control systems in the U.S. energy sector will be able to withstand “an intentional cyber assault with no loss of critical function in critical applications.”<sup>169</sup> This roadmap merely functions as a framework of goals and milestones for protecting control systems, with no authority to enforce or promote these goals.<sup>170</sup> The roadmap also provides a drawn-out ten-year timetable for accomplishment of these goals.<sup>171</sup> Thus, the DHS does not have

165. Homeland Security Act of 2002 § 223, 6 U.S.C. § 143 (2006).

166. U.S. DEP'T OF HOMELAND SEC., *supra* note 43, at ix; U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 115 (2009) (describing the role of the DHS as “[p]roviding technical assistance to other governmental entities and the private sector with respect to emergency recovery plans”).

167. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 43, at 14-15 (describing the narrow way in which the DHS has interpreted its grant of authority under statutes and executive orders, e.g., “[o]ur traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts” and “[b]road regulations mandating how all corporations must configure their information systems could divert more successful efforts by creating a lowest-common denominator approach to cybersecurity.”).

168. U.S. DEP'T OF ENERGY & U.S. DEP'T OF HOMELAND SEC., *supra* note 115.

169. *Id.* at 1.

170. *See id.* at 2.

171. *Id.*

authority to regulate NUSP-consumer cyber security concerns on its own. Instead its function is largely one of aiding agencies to develop their own standards.

*B. Only PUCs or the FTC's State Analogues Have Authority to Regulate NUSP-Consumer Privacy Concerns*

The FERC, the FCC, PUCs, and the FTC and its state analogues are all entities that have some authority to regulate NUSP-consumer privacy concerns. This Section explains why the FERC, the FCC, and the FTC are currently unable to regulate these concerns. It then explains why PUCs and the state analogues of the FTC may be able to do so.

1. The FERC

Under the current regulatory framework, the FERC has authority to adopt the interoperability and functionality standards developed by the NIST.<sup>172</sup> The FERC has interpreted this authority to include the ability to apply these standards to entities all the way down to the retail level.<sup>173</sup> Thus, because the NIST has determined that interoperability and functionality standards should include privacy standards, the FERC has the authority to adopt privacy standards that apply to entities all the way down to the retail level. Further, because NUSPs are retail-level entities that interact directly with consumers, the FERC has the authority to regulate the privacy aspects of NUSP-consumer interactions. However, this regulatory authority is inadequate for proper regulation of NUSP-consumer privacy concerns because it does not include the authority to mandate the adoption of these standards or to enforce them. Accordingly, in order to ensure that the FERC can adequately regulate the privacy aspects of NUSP-consumer interactions, federal legislation must be passed to give the FERC these authorities.

2. The FCC

As noted above, the ARRA gave the FCC new authority to establish an NBP to advance energy independence and efficiency.<sup>174</sup> Although some organizations requested that the FCC take an active role in regulating the privacy aspects of the smart grid via this authority,<sup>175</sup> in

---

172. *See supra* text accompanying note 118.

173. *See* Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

174. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 6001(k)(2)(D), 123 Stat. 115 (to be codified at 47 U.S.C. § 1305); *see also* FED. COMM'NS COMM'N, *supra* note 160, at 1.

175. *See generally* ELEC. PRIVACY INFO. CTR, A NATIONAL BROADBAND PLAN FOR OUR FUTURE (2009) (advocating that the FCC “[s]hould [p]ursue a [w]ide [r]ange of [a]pproaches . . . to [a]ddress [b]roadband [p]rivacy”).

the NBP the FCC only noted that “many users are increasingly concerned about their lack of control over sensitive personal data” and warned that “[i]nnovation will suffer if a lack of trust exists between users and the entities with which they interact over the Internet.”<sup>176</sup> The FCC then made several recommendations, but, as with cyber security concerns, passed on taking a more active role in regulating privacy concerns with the smart grid.<sup>177</sup> As a result, the FCC will likely not be able to regulate NUSP-consumer privacy concerns unless it takes a more active role under its ARRA authority.

### 3. The FTC, Its State Analogues, & PUCs

Because the FTC and its state analogues are the primary government agencies with jurisdiction over consumer protection,<sup>178</sup> these are currently the only government entities that may regulate the privacy aspects of NUSP-consumer interactions.

The FTC is charged with protecting consumers from “unfair and deceptive acts or practices in or affecting commerce.”<sup>179</sup> The FTC has interpreted this to cover privacy concerns<sup>180</sup> and has recognized the need for protection of consumer privacy at least since 1996.<sup>181</sup> In protecting consumers, the FTC has pursued a policy of self-regulation for cyber commerce in which the only guidelines for regulated entities are the FTC’s Fair Information Practice Principles (“FIPPs”).<sup>182</sup> These principles require entities to (1) notify consumers of the entity’s information practices, (2) receive consent from consumers regarding the information practices, (3) allow consumers to access the information that the entity has on them, (4) secure the consumers’ information, and (5) allow consumers to seek redress to enforce the entity’s promises regarding the consumers’ information.<sup>183</sup> Although the FTC’s official policy is self-regulation, the FTC has been actively enforcing the promises of self-regulated entities to consumers through the courts for

176. FED. COMM’NS COMM’N, *supra* note 161, at 53.

177. *Id.* at 55-57.

178. Some other agencies have a consumer protection role to some extent although it is not their main purpose. For example, the U.S. Environmental Protection Agency controls labeling requirements for pesticides.

179. The Federal Trade Commission Act of 1914, 15 U.S.C. § 45(a)(1) (2006).

180. *See, e.g.*, FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 33 (2000); FED. TRADE COMM’N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE 30 (2008).

181. *See, e.g.*, FED. TRADE COMM’N, ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE 35 (1996).

182. Joseph Tarrow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3:3 J.L. & POL’Y FOR INFO. SOC’Y 723, 727-28 (2007).

183. *Fair Information Practice Principles*, FED. TRADE COMM’N, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm> (last modified June 25, 2007).

over ten years.<sup>184</sup> For example, the FTC has brought suit and obtained settlement from numerous companies that have compromised the financial and/or medical data security of customers.<sup>185</sup> These enforcement actions suggest that the FTC has authority to regulate privacy violations occurring within NUSP-consumer interactions. However, under the FTC's current policy of self-regulation, this authority would not necessarily protect consumers from privacy violations because it would only provide consumers with recourse after their privacy had been violated. In effect, the only protection consumers would receive is some difficult-to-measure degree of protection resulting from the deterrent effect that the threat of suit by the FTC would have on companies. Accordingly, the FTC may have authority to regulate NUSP-consumer privacy concerns. However, it is likely that this level of regulation would be inadequate for preventing privacy violations under the current agency policy of self-regulation.

In addition to the FTC, many states have either a PUC or a separate consumer protection agency enforce state privacy laws.<sup>186</sup> These laws may not be inconsistent with the federal unfair and deceptive trade practice laws that established the FTC. However, the Supreme Court has affirmed the authority of states to establish privacy safeguards that provide stronger consumer protections than federal laws.<sup>187</sup> Accordingly, states may pass laws to regulate NUSP-consumer privacy concerns either through the PUC or the state consumer protection agency. Currently, as found by the NIST through developing interoperability and functionality standards, most state PUCs lack formal privacy policies or standards related to the smart grid, and state privacy laws generally do not address privacy concerns related to the smart grid.<sup>188</sup> Thus, while states have the ability to regulate these privacy concerns, legislation must be passed or regulations must be developed by states to adequately address NUSP-consumer privacy concerns.

---

184. *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 8, 9 n.17 (2010) (describing enforcement actions taken by the FTC under Section 5 of the Federal Trade Act and listing examples of such cases going back to 1999).

185. *Id.* at 47 & n.20

186. *See* NISTIR DRAFT FEB. 2010, *supra* note 15, at 103.

187. *See* *Altria Group, Inc. v. Good*, 129 S.Ct. 538, 551 (2008) (holding that state law predicated on a duty not to deceive is not impliedly preempted by various FTC decisions); *Am. Bankers Ass'n v. Lockyer*, 541 F.3d 1214, 1218 (9th Cir. 2008) (holding that some provisions of a California consumer protection law should be held valid even though other provisions were preempted by federal law).

188. *Id.*

#### IV. WHICH ENTITY SHOULD REGULATE NUSP-CONSUMER INTERACTIONS?

No government entity has authority to adequately regulate NUSP-consumer cyber security concerns, and although PUCs and the state analogues of the FTC have authority to regulate NUSP-consumer privacy concerns, very few are taking steps to do so.<sup>189</sup> Accordingly, this Part evaluates which government entities would be the optimal choices for regulating NUSP-consumer cyber security and privacy concerns. In making these determinations, the following factors are evaluated as crucial considerations: (1) areas of expertise within government entities, (2) ability to achieve efficiency gains from the streamlining of government functions (e.g. speed in implementing regulation and reduction in regulatory complexity), and (3) likelihood of encountering undesirable side-effects from giving a government entity regulatory authority (e.g. piecemeal regulation and externalities). As such, Section A considers each potential regulator in turn and explains why the FERC should be given authority to regulate NUSP-consumer cyber security concerns. Then, Section B considers each potential regulator in turn and explains why the FERC should also be given authority to regulate NUSP-consumer privacy concerns.

##### *A. The FERC Should Regulate NUSP-Consumer Cyber Security Concerns*

###### 1. PUC Regulation Is Not Ideal

While PUCs may have the most expertise for handling localized issues like NUSP-consumer interactions, PUCs are not the best entities to regulate NUSP-consumer cyber security concerns for several reasons: (1) PUC regulation could only be achieved by states individually passing legislation to create this authority, which would not streamline government function and may not be possible due to preemption and Dormant Commerce Clause concerns; and (2) PUC regulation would inevitably lead to undesirable side-effects such as piecemeal regulation and negative externalities between states.

One strong argument for PUC regulation of NUSP-consumer cyber security concerns is that PUCs have the most expertise in handling localized interactions related to the electric grid, such as NUSP-consumer interactions. NUSP-consumer interactions are localized interactions, and PUCs likely have the most expertise in handling localized interactions via experience regulating the retail electricity

---

189. See *supra* Part II.B.2.

market.<sup>190</sup> This argument assumes that a PUC's knowledge and experience gathered from regulating intrastate retail utility-consumer interactions translates to an advantage in regulating NUSP-consumer interactions. This assumption may be accurate because experience regulating localized interactions is likely to have given the PUC the resources and know-how needed to effectively implement other localized regulations, including regulations related to NUSP-consumer cyber security concerns.<sup>191</sup> Accordingly, it can be argued that regulation by an entity less familiar with localized interactions is likely to be less effective than regulation by a PUC. Less effective regulation could result in delay. It could also result in incomplete, and, consequently, ineffective implementation of regulation, which could lead to completely inadequate cyber security protection. Although this argument is persuasive, it is heavily outweighed by other considerations.

PUCs are poorly suited to regulate NUSP-consumer cyber security concerns because the state statutes that set out PUC regulatory authority do not currently authorize the regulation of these NUSP-consumer interactions,<sup>192</sup> which means that new legislation must be individually passed by states to authorize this regulatory power.<sup>193</sup> This is problematic for multiple reasons. Most importantly states may not have the legal authority to implement such legislation. Congress has already provided the FERC with jurisdiction through the EISA to implement interoperability and functionality standards, which the FERC has interpreted to cover NUSP-consumer interactions.<sup>194</sup> As a result, it is likely that the FERC's interpretation of this delegation may preempt any state legislation that delegates to PUCs the authority to also regulate cyber security concerns under the Supremacy Clause.<sup>195</sup> Additionally, under *Chevron v. Natural Resources Defense Council* a state challenge to the FERC's interpretation of the EISA could easily fail because a reviewing court would give the FERC substantial deference in interpreting the statute if it were held that the statute's language is ambiguous.<sup>196</sup> Lastly, the state would need to be careful in drafting its legislation so that the authority to regulate these interactions did not place undue burden upon out-of-state NUSPs,

---

190. See *supra* Part III.A.2.

191. See *id.*

192. See, e.g., Joint Comments of the Ctr. for Democracy & Tech. & the Elec. Frontier Found., to the *Order Instituting Rule Making*, RM No. 08-12-009, at 21 (Mar. 9, 2010), available at [http://www.cdt.org/files/pdfs/20100309\\_smartgrid\\_cpuc\\_comments.pdf](http://www.cdt.org/files/pdfs/20100309_smartgrid_cpuc_comments.pdf) (noting that the ability for the California PUC to implement security measures is restricted to "regulable entities" of which this comment posits NUSPs are not).

193. See *supra* notes 135-36 and accompanying text.

194. See Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

195. U.S. CONST. art. VI, cl. 2.

196. *Chevron, U.S.A. v. Natural Res. Def. Council*, 467 U.S. 837, 843-44 (1984).

thereby potentially violating the Dormant Commerce Clause.<sup>197</sup>

Even assuming that state legislation could be passed and upheld, it is undesirable for states to regulate these interactions because PUC regulation may cause detrimental side-effects. For instance, if PUCs were given regulatory authority over NUSP-consumer cyber security concerns, there would be a risk of creating a piecemeal system of regulation. This could result if not all states decided to create PUC authority over these concerns, or if all states did create this authority but did so at different times or to varying degrees. In such a situation, a piecemeal system of regulation would be created. This is problematic because piecemeal regulation of cyber security could lead to negative externalities between states using an interconnected electric grid. In other words, the decision of one state to regulate NUSP-consumer cyber security concerns could be undermined by the decision of another state to forego such regulation. This could result via a security breach occurring in the state without regulation, which negatively affects the state with regulation due to the nature of an interconnected electric grid. This scenario is particularly relevant to cyber security issues because a person seeking to breach security will invariably seek out the easiest way to do so. Moreover, these issues do not disappear when both states decide to regulate. In such a situation it is still possible, and likely, that the two states will have different amounts of resources and expertise that can be put towards regulating these interactions, which may create the same externalities.<sup>198</sup>

Besides the larger issues already addressed, there are also a variety of practical problems that could result from individual states creating this regulatory authority for PUCs. These include the slow speed of the legislative process, difficulties with party politics, the legislative process's vulnerability to lobbying (which could result in watered-down or ineffective legislation),<sup>199</sup> and statutory language that could unintentionally impede the PUC's regulatory flexibility if drafted too narrowly.<sup>200</sup> Finally, extending the jurisdiction of the PUC to entities that are not public utilities is a step that states may be unwilling to take because states may feel that extending jurisdiction to regulate NUSPs is too much like extending jurisdiction to regulate private businesses. Some states might consider this to be an overreaching of regulatory authority because PUCs conventionally regulate only public utilities.<sup>201</sup>

---

197. U.S. CONST. art I, § 8, cl. 3.

198. Robert W. Hahn et al., *Federalism and Regulation*, 2004 REGULATION 46, 47.

199. Email from Elias Leake Quinn, Former Senior Policy Analyst, Ctr. for Envtl. & Energy Sec., Univ. of Colo. Law Sch., to author (Jan. 10, 2010) (on file with the Journal on Telecommunications and High Technology Law).

200. *Id.*

201. See *supra* notes 148-50 and accompanying text.

## 2. DOE Regulation Is Not Ideal

The DOE has significant technical expertise regarding cyber security issues, it has some responsibility to regulate smart grid development, and it is involved with NIST in creating smart grid interoperability and functionality standards.<sup>202</sup> Ultimately, however, the DOE should not be given authority to regulate NUSP-consumer cyber security concerns because (1) this would unnecessarily complicate the electric regulatory framework, and (2) the DOE's technical expertise would be better used for assisting in regulation. Further, the DOE may not want to assume this regulatory responsibility.

The DOE has extensive experience developing security standards for energy control systems.<sup>203</sup> This experience includes: identifying cyber vulnerabilities in energy control systems, working with vendors to develop hardened systems that mitigate cyber security risks, developing more secure communication methods between energy control systems and field devices, developing tools and methods to help utilities assess their security posture, and providing extensive cyber security training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.<sup>204</sup> This expertise was the reason that the NIST was required to collaborate with the DOE in creating interoperability and functionality standards.<sup>205</sup> However, despite this expertise, it would be undesirable to give the DOE authority to regulate NUSP-consumer cyber security concerns because this would further complicate the electric regulatory framework—something that desperately needs to be streamlined for the smart grid.

Giving the DOE the power to regulate NUSP-consumer interactions would create a new facet to electric regulation outside of the traditional FERC-PUC regulatory scheme and the new interoperability and functionality authority of the FERC. This facet would unnecessarily complicate regulation because the resultant regulatory framework would require the FERC to adopt security standards, but would then charge the DOE with the responsibility to enforce them. This could cause jurisdictional blurring down the road, which, as this Note illustrates, creates uncertainty and can impede regulatory action.<sup>206</sup> Instead of

---

202. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 2.

203. See U.S. DEP'T OF ENERGY, *supra* note 60, at 2.

204. *Id.*

205. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 4.

206. See, e.g., Comments of the Nat'l Ass'n of Regulatory Util. Comm'rs, to the *Proposed Policy Statement & Action Plan*, in Smart Grid Policy, Dkt. No. PL09-4-000, at 1 (May 11, 2009), [available at](http://www.naruc.org/Testimony/09%200511_NARUC%20Comments%20on%20FERC%20DRAFT%20POLICY%20STATEMENT.pdf) [http://www.naruc.org/Testimony/09%200511\\_NARUC%20Comments%20on%20FERC%20DRAFT%20POLICY%20STATEMENT.pdf](http://www.naruc.org/Testimony/09%200511_NARUC%20Comments%20on%20FERC%20DRAFT%20POLICY%20STATEMENT.pdf) (noting that the FERC's Smart Grid Policy Statement's assertions raise jurisdictional issues that must be resolved to proceed effectively).

creating confusion, uncertainty, and complicating regulation, it would be vastly more beneficial to streamline regulatory authority and jurisdictional boundaries (especially for the already confusing regulatory landscape of smart grid development). Perhaps a more preferable role for the DOE would be one similar to that which it occupies for the NIST standards: the DOE could serve as an adviser to the FERC on technical cyber security issues that may arise during regulation of NUSP-consumer cyber security concerns. Under this scenario the DOE would still be able to offer its expertise to secure the grid from these concerns, but the regulatory framework would not become more complicated.

Lastly, it is possible that the DOE may not want to regulate NUSP-consumer cyber security concerns. The Assistant Secretary for the Office of Electricity Delivery and Energy Reliability at the DOE has testified before the House Subcommittee on Energy and Environment regarding the DOE's "recommended courses of action" for dealing with security issues associated with smart grid development.<sup>207</sup> Nowhere in those recommendations were calls for legislation or delegation of additional authority to the DOE.<sup>208</sup>

### 3. FCC Regulation Is Not Ideal

Like the DOE and the DHS (as discussed below), the FCC has agency expertise that may be helpful in regulating NUSP-consumer cyber security concerns. However, the FCC has no experience regulating the electric grid. Consequently, it is counterintuitive and out-of-place to put it in charge of regulating these concerns because the FCC's involvement in regulating the grid would lead to increased regulatory complexity and decreased efficiency. Although the FCC may play a role in assisting the more traditional regulatory players via its NBP and ARRA authority, the FCC would not be the optimal choice for regulating NUSP-consumer cyber security concerns.

### 4. DHS Regulation Is Not Ideal

Although the DHS has some responsibility for addressing cyber security concerns, it is not the proper entity to regulate these interactions because the DHS has expertise in aiding other agencies with cyber security concerns but no experience in implementing cyber security standards. As a result, DHS regulation could lead to ineffective implementation of cyber security standards.

---

207. See *Effectively Transforming Our Electric Delivery System to a Smart Grid: Hearing Before the Subcomm. on Energy & Env't of the H. Comm on Sci. & Tech.*, 111th Cong. 15-16 (2009) (statement of Patricia Hoffman, Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability, Dep't. of Energy).

208. *Id.*

As noted above,<sup>209</sup> the role of the DHS in developing cyber security standards has largely been one of aiding agencies to develop their own standards rather than controlling the creation and implementation of standards. This is significant because this traditional function likely means that the DHS has significant agency expertise in helping agencies decide what types of standards to implement but no actual expertise in implementing such standards itself. Thus, the DHS would likely require more time to obtain the necessary personnel to adequately regulate NUSP-consumer cyber security concerns than other agencies that already have staffs with such regulatory experience. Consequently, for efficiency and efficacy reasons, it is beneficial to give authority to regulate NUSP-consumer cyber security concerns to a government entity that can assume this responsibility with less effort.

### 5. FERC Regulation Is Optimal

The FERC should regulate NUSP-consumer cyber security concerns because (1) federal regulation would avoid preemption and piecemeal regulation issues related to state regulation, (2) FERC regulation would contribute to streamlined regulation of the smart grid, which would in turn lead to more efficient and perhaps more effective regulation, (3) the FERC has expertise in implementing and enforcing regulatory standards on the grid via its EPCRA of 2005 reliability authority, and (4) FERC regulation would be the simplest option, requiring the passage of minimal legislation or reinterpretation of the FERC's interoperability and functionality standards authority under the EISA.

As noted above, leaving the regulation of NUSP-consumer cyber security concerns to states may not be possible and, if possible, may result in ineffective regulation. Accordingly, federal regulation is more appropriate for NUSP-consumer cyber security concerns. Of the federal entities that could regulate NUSP-consumer cyber security concerns, the FERC is the best suited because it already has experience developing cyber security standards to address these concerns.<sup>210</sup> As a result, the FERC has personnel and resources already allocated to this area, allowing the agency to assume this additional authority with minimal effort.<sup>211</sup>

---

209. See *supra* Part III.A.5.

210. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 4; Smart Grid Policy, 74 Fed. Reg. 37,098 (July 16, 2009).

211. For example, the FERC has a smart grid webpage, a smart grid policy statement, and various other policy documents and congressional testimonies dedicated to addressing the role of the FERC and its involvement in the interoperability and functionality standards, including their cyber security standards aspect. *Smart Grid*, *supra* note 8 (select links under "Quick Links").

Deciding to delegate this authority to the FERC would also concentrate regulatory authority in the FERC instead of unnecessarily dividing it among other agencies. Concentrating authority in the FERC would be beneficial because it would streamline federal regulation of the smart grid, thus creating clearer departmental roles, and, subsequently, increased regulatory efficiency and effectiveness. This may happen because clearer departmental roles reduce uncertainty as to which government agency will regulate. And this, in turn, is beneficial for several reasons. First, it reduces the need for regulators to make difficult and time-consuming jurisdictional decisions. Second, because regulated entities know more quickly and with greater certainty which regulators have authority, regulated entities, too, can act more quickly and with greater faith that they will not face unanticipated regulatory requirements.

Furthermore, streamlining of federal regulation will reduce complexity and confusion in the regulatory framework.<sup>212</sup> The value of this effect has been noted implicitly by the statements of cyber security experts, who caution about the current “lack of transparency and dearth of defined departmental roles and responsibilities in addressing cyber-related issues from a comprehensive national approach.”<sup>213</sup> Lastly, streamlining can increase regulatory efficiency by helping to avoid vulnerabilities in regulation caused by inconsistent regulations from multiple agencies.<sup>214</sup> Thus, extending the FERC’s jurisdiction to regulate NUSP-consumer cyber security concerns is desirable because it can lead to increased regulatory efficiency and efficacy.

Finally, allowing the FERC to regulate NUSP-consumer cyber security concerns would require less effort than creating a new authority for a different federal agency. To allow the FERC to regulate these concerns would either require the passage of minimal legislation extending the FERC’s current interoperability and functionality standards authority under the EISA, or it would require the FERC to

---

212. Regulatory streamlining is commonly pursued when trying to achieve regulatory efficiency, cost-effectiveness, and regulatory certainty. For instance, streamlining efforts pursued by U.S. federal agencies include streamlining of the regulation of construction, both generally and for nuclear power. *See, e.g.*, NAT’L P’SHIP TO STREAMLINE GOV’T, <http://www.natpartnerstreamline.org> (last visited Feb. 11, 2011) (noting enormous cost savings and increased efficiency as a result of streamlining efforts in the regulation of general construction); DEP’T OF ENERGY, THE ECONOMIC FUTURE OF NUCLEAR POWER: A STUDY CONDUCTED AT THE UNIVERSITY OF CHICAGO (2004) (describing streamlining of the nuclear power permitting process).

213. CATHERINE A. THEOHARY & JOHN ROLLINS, CONG. RESEARCH SERV., CYBERSECURITY: CURRENT LEGISLATION, EXECUTIVE BRANCH INITIATIVES, AND OPTIONS FOR CONGRESS 7 (2009).

214. *Id.* at 7-8.

reinterpret this existing authority.<sup>215</sup> These options are simpler to accomplish than passing legislation to create an entirely new function for a different agency.<sup>216</sup> For instance, although numerous factors contribute to the difficulty in passing legislation, it is arguable that extending the regulatory authority of an agency that nearly enjoys this authority already is easier to achieve than obtaining consensus that a bill should be passed to allow an agency with less regulatory authority in that area to have wholly new powers. Thus, for the foregoing reasons, the FERC is the optimal choice for regulation of NUSP-consumer cyber security concerns.

### *B. The FERC Should Regulate NUSP-Consumer Privacy Concerns*

Although the FTC and its state analogues are the traditional government agencies with jurisdiction over consumer protection, and although these entities and PUCs may regulate NUSP-consumer privacy concerns after taking certain steps,<sup>217</sup> the FERC is best suited to regulate these concerns. FERC regulation is the optimal choice because (1) the FERC has more experience regulating the electric grid than the FTC or state analogues, (2) the FERC has experience mandating and enforcing standards from its reliability authority, (3) PUCs are likely to encounter piecemeal regulation issues, and (4) allocating regulatory authority to the FERC will streamline federal regulation of the smart grid. Thus, either the FERC should reinterpret its interoperability and functionality standards authority to include the authority to mandate and enforce the privacy standards for the smart grid being developed by the NIST, or federal legislation should be passed to give the FERC this authority.

The FERC has decades of experience regulating the electric grid, whereas the FTC and its state analogues have no experience regulating the grid.<sup>218</sup> Expertise translates into a better ability to regulate because agencies with expertise better understand what manner of regulation works best. In addition, agencies with expertise do not need to familiarize themselves with an area of regulation, allowing them to implement regulation more quickly than agencies with less expertise.

---

215. See *Smart Grid Initiatives and Technologies*, *supra* note 53, at 2; Smart Grid Policy, 74 Fed. Reg. 37,098 & 37,101 (July 16, 2009).

216. This argument assumes that political feasibility is lower when legislation with a broad, as compared to a narrow, purpose is needed.

217. As noted in Part III.B.3, the FTC would need to change its policy of self-regulation to actively regulate these concerns, and the states would need to either allow their PUCs to enact regulations to control NUSP-consumer privacy concerns or pass legislation allowing the state's consumer protection agencies to take on that responsibility.

218. See *Students' Corner, What is FERC?*, U.S. FED. ENERGY REG. COMM'N, <http://www.ferc.gov/students/whatisferc/history.htm> (explaining that FERC regulation dates back to the formation of the predecessor of the FERC, the Federal Power Commission, in 1920) (last visited Feb. 11, 2011).

Because the smart grid is complex and is developing quickly, effective and timely regulation is crucial. Thus, one reason that the FERC is a better choice than the FTC or its state analogues for regulating NUSP-consumer privacy concerns is that it is likely to be better able to keep pace with smart grid development.

It is also preferable to give the FERC authority to regulate NUSP-consumer privacy concerns rather than the FTC or its state analogues because the FERC has related experience mandating and enforcing standards from its reliability authority under the EAct of 2005.<sup>219</sup> Experience enforcing standards makes the FERC a strong candidate for similar regulatory authority because the FERC could simply adjust its current enforcement practices to include these additional standards. However, the FTC or its state analogues might have more difficulty adjusting to a regulatory role that they are less familiar with fulfilling.

The FERC is a preferable entity for regulating NUSP-consumer privacy concerns because in exercising this authority, the FERC acts as a single entity and therefore will not run into piecemeal regulation issues. Piecemeal regulation is particularly problematic when unified policy is needed for effective regulation. In the case of cyber security, this is a paramount concern because cyber security of the grid is dependent upon effective regulation of the entire grid. It is unclear whether or not piecemeal regulation of NUSP-consumer privacy concerns presents the same degree of danger to the privacy of all users of the grid. However, common sense advises that in deciding how to best regulate these privacy concerns, it is better to err on the side of caution and avoid piecemeal regulation. This may be preferable due to the interconnected nature of the grid and networks that are the hallmark of the smart grid. Additionally, in consideration of the rapid speed of smart grid technology development, it is likely more sensible to seek uniform regulation and avoid needing to re-delegate authority at a later time due to a later-found shortcoming of piecemeal regulation.

Lastly, in the same vein as the analysis of cyber security regulation, it is prudent to consider how tangential authorities are allocated when deciding how to delegate regulatory authority over privacy concerns. The FERC is the optimal choice for regulating NUSP-consumer cyber security concerns via its interoperability and functionality standards authority. However, the interoperability and functionality authority extends to privacy concerns as well. Accordingly, it may be disadvantageous to allow the FERC to regulate the cyber security aspects of NUSP-consumer interactions, but to not regulate these interactions' privacy aspects. For example, a decision to aggregate or streamline

---

219. *Office of Enforcement*, FED. ENERGY REG. COMM'N, <http://www.ferc.gov/about/offices/oe.asp> (last updated Feb. 25, 2011).

regulatory authority over the smart grid rather than to divide it among multiple agencies might increase efficiency by reducing regulatory complexity. Complexity not only makes it difficult for regulated entities to understand what authorities they report to, but it also makes it difficult for regulators to act because regulatory actions will require difficult jurisdictional decisions. Thus, in the interest of streamlining the federal government regulation of the smart grid, this authority should be delegated to the FERC.

## CONCLUSION

NUSP-consumer interactions pose a danger to the security of the electric grid and to the privacy interests of its users. Because no government entity currently has the authority to effectively regulate these interactions, regulatory authority must be extended to cover them. The FERC is the most attractive candidate to assume this authority because it already has the power to promulgate non-compulsory standards for NUSP-consumer cyber security and privacy concerns under its interoperability and functionality standards authority. Accordingly, either the FERC should reinterpret its interoperability and functionality standard authority to encompass the ability to mandate or enforce the NIST's cyber security and privacy standards, or legislation should be passed to extend this authority to the FERC. Failing to address these concerns will likely result in the continued ineffectual regulation of NUSP-consumer interactions. Such ineffectual regulation could potentially result in the invasion of consumer privacy interests or the endangerment of the electric grid—things that unarguably should be avoided.



# A RESEARCH REVOLUTION: GENETIC TESTING CONSUMERS BECOME RESEARCH (AND PRIVACY) GUINEA PIGS

ANGELA L. MORRISON\*

|   |     |
|---|-----|
| INTRODUCTION .....  | 574 |
| I. BACKGROUND .....   | 574 |
| <i>A. Regulation of Human Subject Research in the United States</i> ...                   | 575 |
| 1. Historical Examples of Abuse.....  | 575 |
| 2. Current Laws .....   | 576 |
| <i>B. Human Genome Sequencing and Testing</i> .....                                       | 578 |
| 1. Sequencing the Human Genome .....  | 578 |
| 2. Direct-to-Consumer Genetic Testing.....  | 579 |
| II. ONLINE COMMUNITIES AS A SOURCE OF<br>HUMAN SUBJECTS FOR GENETIC RESEARCH.....         | 580 |
| <i>A. Research Arms of Direct-to-Consumer Genetic Testing<br/>        Companies</i> ..... | 580 |
| <i>B. Non-Profit Research Consortiums</i> .....   | 581 |
| III. GENETIC INFORMATION PRIVACY IN ONLINE<br>RESEARCH COMMUNITIES .....                  | 582 |
| <i>A. Relevant Legislation</i> .....  | 583 |
| 1. The Genetic Information Nondiscrimination Act of<br>2008 .....                         | 583 |
| 2. State Laws.....  | 584 |
| <i>B. Privacy Policies, Terms of Service, and Informed Consent</i> .....                  | 585 |
| 1. Direct-to-Consumer Genetic Testing Companies.....                                      | 585 |
| 2. Non-Profit Research Consortiums .....  | 588 |
| IV. PRIVACY VERSUS PUBLIC BENEFIT .....   | 590 |
| <i>A. Privacy Concerns</i> .....  | 590 |
| 1. Reidentification: The Loss of Anonymity .....  | 590 |
| 2. Informed Consent and Autonomy .....  | 592 |
| 3. Genetic Discrimination .....   | 593 |
| <i>B. Public Benefit: Promoting, Not Impeding, Genetic Research</i> ...                   | 593 |
| <i>C. Balancing Concerns</i> .....  | 595 |

---

\* J.D., University of Colorado Law School (2011); M.S., Colorado State University (2007).

|    |  |     |
|----|--|-----|
| V. | RECOMMENDATIONS.....   | 596 |
| A. | <i>Addressing Reidentifiability</i> .....                              | 596 |
| B. | <i>Legislative Reform</i> .....  | 597 |
|    | 1. Expansion of the Genetic Information<br>Nondiscrimination Act ..... | 597 |
|    | 2. Revising the Common Rule .....                                      | 598 |
| C. | <i>Protective Approaches</i> .....                                     | 601 |
|    | 1. Stewardships .....  | 601 |
|    | 2. Certificates of Confidentiality .....                               | 602 |
| D. | <i>Interactive Informed Consent</i> .....                              | 603 |
|    | CONCLUSION .....   | 605 |

## INTRODUCTION

Direct-to-consumer genetic testing companies, which offer DNA sequencing services to paying customers, and publicly-funded genetic research consortiums have both begun to conduct Internet-based genetic research studies. The offered levels of privacy and anonymity vary greatly, but even those entities that promise maximum privacy protection can no longer guarantee much, as investigators recently revealed how easy it is to identify a given individual from “anonymized” data. Prohibiting these reidentification events is unlikely to be effective, but prohibition on the opposite end (participation in research) is undesirable because individuals, the research community, and the public at large benefit from scientific and medical discoveries achieved through research. And yet, if study participants fear the consequences of participation, such as genetic discrimination or loss of control of their information and its dissemination (e.g. being identified as a Huntington’s disease carrier when you had chosen not to tell anyone), participation will decrease. Because we cannot stop the advancements in computer science that enable reidentification, it is time to update existing protections for traditional human research subjects in order to meet the demands of the rapidly advancing online research community, specifically via open and interactive informed consent.

## I. BACKGROUND

Advances in human science and medicine are often dependent upon research on human subjects. Shameful experiments on humans, not only in the oft-cited Nazi Germany, but also in the United States, lead to regulations on human subject research and protections for the participants. Since then, rapid developments in the fields of genetics and genomics along with the rise of an Internet society have greatly expanded

the breadth of topics on which human subject research can be conducted and the forums in which that research can take place. This section provides some background on human subject research and its regulation, and on genetic sequencing and its availability online.

### *A. Regulation of Human Subject Research in the United States*

#### 1. Historical Examples of Abuse

In July of 1972, an Associated Press journalist broke the story of a United States Public Health Service study, then in its fortieth year, on the effects of untreated syphilis.<sup>1</sup> The Tuskegee Study involved 399 syphilitic African American men in rural Macon County, Alabama who apparently did not know they had syphilis or knew, but did not know they were not receiving treatment for it.<sup>2</sup> Instead, they were receiving free medical examinations, hot meals, and a burial stipend for participation in a study in which researchers simply let syphilis run its course in order to investigate the ultimately fatal effects of the disease.<sup>3</sup> It appeared that government researchers had taken advantage of poor, illiterate men by misleading them into believing they were receiving proper medical attention.<sup>4</sup>

Not long before the Tuskegee story broke, researchers in New York completed a decade-long study on the effects of viral hepatitis.<sup>5</sup> The study subjects were residents of Willowbrook State School, a now-defunct institution for mentally challenged children.<sup>6</sup> Researchers intentionally infected some of the children in order to study controlled progression of the disease.<sup>7</sup> The investigators justified their work by pointing out that viral hepatitis was endemic in the institution, and deliberate infection with a mild strain conferred immunity against more virulent strains.<sup>8</sup> They also obtained consent for the artificial induction from the residents' parents.<sup>9</sup> Opponents denounced using children in

---

1. JAMES H. JONES, *BAD BLOOD: THE TUSKEGEE SYPHILIS EXPERIMENT 1* (new & expanded ed. 1993).

2. *Id.* at 5-6.

3. *Id.* at 4.

4. *Id.* at 13-14.

5. See generally Saul Krugman, Joan P. Giles & Jack Hammond, *Infectious Hepatitis: Evidence for Two Distinctive Clinical, Epidemiological, and Immunological Types of Infection*, 200 JAMA 365 (1967) (providing background information about hepatitis at Willowbrook and describing several of the studies).

6. *Id.* at 366.

7. *Id.*

8. Saul Krugman, Letter to the Editor, *Experiments at the Willowbrook State School*, 297 LANCET 966, 966-67 (1971).

9. Krugman et al., *supra* note 5, at 366.

medical research, especially the mentally impaired.<sup>10</sup> They also argued that consent was in effect coerced because when the main unit of the institution refused to accept new patients (due to alleged overcrowding), the separate research unit, reserved for study participants only, continued to welcome residents; thus, the only avenue for admittance was participation in the hepatitis study.<sup>11</sup>

## 2. Current Laws

Public outrage over studies such as those at Tuskegee and Willowbrook drew some unfavorable comparisons to the experiments of Nazi Germany,<sup>12</sup> but at least one of the research directors failed to see any similarity to Nazi abuses or any applicability of the Nuremberg Code to his work.<sup>13</sup> Recommendations regarding the ethical treatment of human subjects in research had actually existed for several decades,<sup>14</sup> but there was almost no federal oversight until the National Research Act of 1974,<sup>15</sup> which was enacted after Tuskegee and Willowbrook. Years of discussions following the 1974 Act were memorialized in the influential Belmont Report,<sup>16</sup> which eventually lead, in 1991, to the Federal Policy for Protection of Human Subjects, more often referred to as the Common Rule.<sup>17</sup>

The Common Rule mandates that researchers at any public or private institution (hospital, clinic, laboratory, etc.) that receives government funding or is otherwise regulated by the government first

10. Stephen Goldby, Letter to the Editor, *Experiments at the Willowbrook State School*, 297 LANCET 749 (1971).

11. M.H. Pappworth, Letter to the Editor, *The Willowbrook Experiments*, 297 LANCET 1181 (1971).

12. JONES, *supra* note 1, at 12.

13. *Id.* at 179-80 (referring to interview with Dr. John R. Heller, director of the Division of Venereal Diseases from 1943-48); Nuremberg Medical Trial, *The Nuremberg Code (1947)*, in CONTEMPORARY ISSUES IN BIOETHICS 70, 70-71 (7th ed. 2008) (reprinting the Nuremberg Code, which lists ten "basic principles [that] must be observed in order to satisfy moral, ethical and legal concepts" of human medical experiments).

14. *See, e.g.*, Minutes of the Supplemental Session of the House of Delegates of the American Medical Association, Held in Chicago, Dec. 9-11, 1946, *reprinted in* Organization Section, 132 JAMA 1075, 1090 (1946).

15. RESEARCH COMPLIANCE SERVS., OFFICE OF RESEARCH, THE HUMAN SUBJECTS RESEARCH REVIEW SYSTEM 1 (2001). The predecessor to the U.S. Department of Health and Human Services, the Department of Health, Education, and Welfare, had issued guidelines on the protection of human subjects just three years earlier, in 1971. *Id.*

16. NAT'L COMM'N FOR THE PROTECTION OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAVIORAL RESEARCH, NAT'L INSTS. OF HEALTH, THE BELMONT REPORT (1979), *available at* <http://ohsr.od.nih.gov/guidelines/belmont.html>.

17. Federal Policy for the Protection of Human Subjects, 56 Fed. Reg. 28,003 (June 18, 1991) (codified in scattered sections of C.F.R.).

seek approval for studies involving human subjects.<sup>18</sup> Approval comes from a local Institutional Review Board (“IRB”), a group of at least five people of diverse backgrounds, including one community member, at least one person whose primary concerns are scientific, and at least one person whose primary concerns are nonscientific.<sup>19</sup> The members must have expertise to review specific research projects, must know the applicable law, and must know the standards of professional practice.<sup>20</sup> No member may review his or her own research proposal.<sup>21</sup>

IRBs can decide to approve, demand modification of, or deny a research proposal involving human subjects.<sup>22</sup> Requisite criteria for an approvable proposal include the following: risks to the subjects are minimized, risks to the subjects are reasonable in relation to the anticipated benefits, selection of subjects is equitable, and informed consent is obtained.<sup>23</sup> Proper informed consent includes a description of risks to the subject, identification of benefits to the subject or to others, and a statement that participation is voluntary and that the subject may withdraw at any time.<sup>24</sup> Additionally, a statement describing the extent of confidentiality of records identifying the participant must be included.<sup>25</sup> The existence of adequate provisions for protecting the privacy of subjects and maintaining confidentiality of data is one of the criteria IRBs consider when they evaluate proposals.<sup>26</sup>

IRBs are not required at institutions that do not receive any federal funding and whose research does not otherwise fall under federal regulation.<sup>27</sup> This means that private pharmaceutical companies *are* subject to IRB approval because a government agency, the Food and Drug Administration (“FDA”), regulates the product of their research—pharmaceuticals.<sup>28</sup> IRB approval is also not required when the research project (even if it is federally funded) is limited to the collection of existing data that is publicly available, or if the subjects cannot be identified “directly or through identifiers linked to the subjects.”<sup>29</sup>

---

18. 45 C.F.R. § 46.101(a) (2010).

19. *Id.* § 46.107(a), (c).

20. *Id.* § 46.107(a).

21. *Id.* § 46.107(e).

22. *Id.* § 46.109(a).

23. *Id.* § 46.111(a).

24. *Id.* § 46.116(a).

25. *Id.* § 46.116(a)(5).

26. *Id.* § 46.111(a)(7).

27. *See id.* § 46.101.

28. *See id.*; 21 C.F.R. §§ 56.101-.115 (2010).

29. 45 C.F.R. § 46.101(b)(4) (2010).

Another relevant law is the Health Information Portability and Accountability Act (“HIPAA”).<sup>30</sup> HIPAA prohibits covered entities—health care providers, health plans, health care clearinghouses—from “us[ing] or disclos[ing] protected health information without an authorization” (meaning, informed consent) from the patient whose information is subject to use or disclosure.<sup>31</sup> However, this prohibition does not apply to “de-identified” information; covered entities may use and disclose personal health information, without restriction, if they first remove eighteen listed identifiers such as name, social security number, and home address.<sup>32</sup> Additionally, no patient consent is required for the use or disclosure of otherwise protected health information if that use or disclosure is for research purposes, although a waiver of consent must first be approved by an IRB or a similar privacy board.<sup>33</sup>

## B. Human Genome Sequencing and Testing

### 1. Sequencing the Human Genome

During the 1990s, the publicly-funded Human Genome Project and the private company Celera raced to sequence the human genome, that is, to report all of the nucleotide “letters” of all of the DNA comprising all 24 chromosomes.<sup>34</sup> The groups jointly announced their first working drafts of the human genome in 2000 and they released approximately 90 percent complete annotated drafts the following year.<sup>35</sup> Additional information has been added ever since. In 2007 the first complete sequence of a single individual’s genome was published.<sup>36</sup>

30. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

31. 45 C.F.R. § 164.508(a)(1) (2010). Health information does include genetic information. 42 U.S.C. § 1320d-9(a) (2006).

32. 45 C.F.R. §§ 164.502(d)(2), 164.514(b)(2) (2010). Alternatively, if a statistician determines that “the risk [of reidentification] is very small,” then the information can be used and disclosed without restriction. *Id.* §§ 164.502(d)(2), 164.514(b)(1).

33. *Id.* § 164.512(i)(1)(i).

34. See generally James D. Watson, *The Human Genome Project: Past, Present, and Future*, 248 SCIENCE 44, 45 (1990) (explaining the project, including that all 22 autosomes plus the X and Y sex chromosomes would be sequenced). Celera joined the race full time in 1999. J. CRAIG VENTER, *A LIFE DECODED: MY GENOME: MY LIFE* 286 (2007).

35. Int’l Human Genome Sequencing Consortium, *Initial Sequencing and Analysis of the Human Genome*, 409 NATURE 860, 875 (2001); J. Craig Venter et al., *The Sequence of the Human Genome*, 291 SCIENCE 1304, 1315 (2001).

36. Samuel Levy et al., *The Diploid Genome Sequence of an Individual Human*, 5 PLOS BIOLOGY 2113, 2114 (2007) (identifying J. Craig Venter as the single DNA donor). The first published DNA sequences had been derived from several anonymous donors. Int’l Human Genome Sequencing Consortium, *supra* note 35, at 865-66; VENTER, *supra* note 34, at 285-86.

## 2. Direct-to-Consumer Genetic Testing

Advancements in sequencing equipment and technology that were developed in conjunction with the sequencing of the human genome soon paved the way for several Internet-based companies to provide genome sequencing services directly to members of the general public. These companies are referred to as direct-to-consumer genetic testing companies (“DTC-GTCs”).<sup>37</sup> For the average individual interested in genealogy or predisposition to a given disease, full sequencing (returning the individual nucleotide letters of one’s entire genome), although rapidly decreasing in cost, is still prohibitively expensive and time-consuming.<sup>38</sup> A less expensive option is exome sequencing, which examines just the exons within genes (which are already only a portion of the entire genome).<sup>39</sup> An even cheaper and faster approach is to examine single nucleotide polymorphisms (“SNPs,” pronounced “snips”). Each SNP involves a single change in our DNA code; one nucleotide may have been substituted for a more common one, an extra nucleotide may have been inserted, or one may have been deleted.<sup>40</sup> More than one million SNPs have already been identified and reported by researchers, and they correspond to both non-clinical (e.g. eye color) and clinical (e.g. sickle cell anemia) traits. By using DNA chip technology, DTC-GTCs can study a million SNPs almost simultaneously.<sup>41</sup>

---

37. See, e.g., 23ANDME, <https://www.23andMe.com> (last visited Feb. 24, 2011); DECODEME, <http://www.decode.me> (last visited Feb. 24, 2011); LUMIGENIX, <http://www.lumigenix.com> (last visited Feb. 24, 2011); NAVIGENICS, <http://www.navigenics.com> (last visited Feb. 24, 2011); PATHWAY GENOMICS, <https://www.pathway.com> (last visited Feb. 24, 2011).

38. Illumina’s full genome sequencing service, available only with a physician’s referral, dropped from \$48,000 in early 2010 to \$19,500 by July of that year. And the company charges just \$9,500 if a physician certifies that sequencing could lead to treatment of that patient’s condition. Randall Parker, *Illumina Full Genome Sequencing Costs Below \$20k*, FUTUREPUNDIT (July 18, 2010, 11:37 AM), <http://www.futurepundit.com/archives/007347.html>. Soon, full genome sequencing may cost one tenth of that. John Markoff, *L.B.M. Joins Pursuit of \$1,000 Personal Genome*, N.Y. TIMES, Oct. 6, 2009, at D2.

39. Pauline C. Ng et al., *Genetic Variation in an Individual Human Exome*, 4 PLOS GENETICS 1, 1 (2008), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2493042/pdf/pgen.1000160.pdf>.

40. See, e.g., Alain Vignal et al., *A Review on SNP and Other Types of Molecular Markers and Their Use in Animal Genetics*, 34 GENETICS SELECTION EVOLUTION 275, 277-78 (2002).

41. *How Does 23andMe Genotype My DNA?*, 23ANDME, <https://www.23andme.com/you/faqwin/chip> (last visited Apr. 3, 2011).

## II. ONLINE COMMUNITIES AS A SOURCE OF HUMAN SUBJECTS FOR GENETIC RESEARCH

Most research studies on humans have traditionally been conducted by, and physically at, institutions such as universities, hospitals, and pharmaceutical companies. For example, a pulmonologist might have invited her cystic fibrosis patients to participate in a study on a new treatment, or a clinical professor might have recruited sets of identical and fraternal twins for a nature-versus-nurture study.

While studies on new surgical methods might still have to be conducted in person on an operating room table, the Internet has greatly expanded the types of research studies that can be conducted without personal interaction between researcher and subject. The pulmonologist could have her cystic fibrosis patients and their families submit DNA samples to an online-based testing company in order to investigate the genetic basis of the disease, and she could also create online surveys to gather information about how her patients respond to a new treatment. Similarly, the twins in the nature-versus-nurture study could submit their DNA samples to an online-based twins' community and answer survey questions there, without ever meeting the professor. The Internet has created a whole new forum for scientific research, and both for-profit and not-for-profit groups are utilizing it.

### *A. Research Arms of Direct-to-Consumer Genetic Testing Companies*

The initial premise of DTC-GTCs was that consumers paid to have a DNA sample sequenced and analyzed for information related to their ancestry, risk of disease, and non-disease traits (e.g. earwax type). More recently, companies have added research opportunities whereby customers can share their purchased genetic information for use in research. For the first time, subjects are paying to be enrolled in research studies.<sup>42</sup>

One of the largest DTC companies, 23andMe, has a research arm called 23andWe for the purpose of investigating the basic causes of disease, developing drugs and other treatments, and predicting an individual's risk of disease.<sup>43</sup> It aims to accomplish these goals by creating a larger pool of samples than can be achieved through typical

---

42. In the typical scenario, research subjects are paid for their participation in a study. Council for International Organization of Medical Sciences (CIOMS), in Collaboration with the World Health Organization (WHO), *International Ethical Guidelines for Biomedical Research Involving Human Subjects (2002)*, in CONTEMPORARY ISSUES IN BIOETHICS, *supra* note 13, at 79.

43. *Consent Document*, 23ANDME, <https://www.23andme.com/about/consent> (last visited Apr. 3, 2011).

location-based clinical trials.<sup>44</sup> Participants contribute their genetic information and answer online surveys, which cover a range of topics from non-clinical traits (e.g. freckles, right- or left-handedness) to serious diseases (e.g. Parkinson's disease, diabetes), as well as less-serious conditions (e.g. migraines, lactose intolerance) and responses to drugs.<sup>45</sup> Two clinical research communities, one for Parkinson's disease and one for sarcoma, have also been established. Those who have been diagnosed with Parkinson's, sarcoma, or related disorders may join the respective community if they pledge to contribute their sequenced DNA and to take online surveys about their experiences with the diseases.<sup>46</sup> 23andMe will then "correlate [customers'] responses to online surveys with their genetic data" in order to conduct research studies.<sup>47</sup>

Although not clearly defined or promoted like 23andMe's 23andWe, Navigenics does have a research arm through which it conducts its own genetic and medical research.<sup>48</sup> Navigenics's customers' genetic information may also be used for external research studies,<sup>49</sup> as is true for the customers of most, if not all, DTC-GTCs.<sup>50</sup>

### *B. Non-Profit Research Consortiums*

Publicly funded research projects aim to advance the understanding

44. *Featured Research*, 23ANDME, <https://www.23andme.com/slideshow/research> (slide 1) (last visited Apr. 3, 2011). Until 2010, 23andMe was also running a program called "Research Revolution" which, like 23andWe, was aimed at creating, via the 23andMe customer base, a large enough data pool such that statistically meaningful research on a particular health condition could be conducted. Customers could donate their genetic information to studies on one or more of ten health problems, which included migraines, epilepsy, multiple sclerosis, and rheumatoid arthritis. Those who were suffering from the conditions were called "patients" and when 1,000 patients had enrolled, 23andMe promised to start a research study using both in-house resources and outside experts. Customers who were not suffering from a particular condition could still sign up as "supporters" of that condition and their genetic information would serve as experimental controls. *Research Revolution*, 23ANDME, <https://www.23andme.com/researchrevolution> (last visited Apr. 1, 2010) (archived copy on file with Journal on Telecommunications and High Technology Law). It appears that 23andWe now encompasses the general themes of Research Revolution, but without customer-directed resource allocation to, or topic selection of, research studies.

45. *Featured Research*, 23ANDME, <https://www.23andme.com/slideshow/research> (slide 2) (last visited Apr. 3, 2011); *Consent Document*, *supra* note 43.

46. *23andMe Parkinson's Community: Strength in Numbers*, 23ANDME, <https://www.23andme.com/pd> (last visited Apr. 3, 2011); *23andMe Sarcoma Community: A Patient-Driven Revolution in Sarcoma Research*, 23ANDME, <https://www.23andme.com/sarcoma> (last visited Apr. 3, 2011).

47. *Featured Research*, *supra* note 44.

48. *See Privacy Policy*, NAVIGENICS, [http://www.navigenics.com/visitor/what\\_we\\_offer/our\\_policies/privacy](http://www.navigenics.com/visitor/what_we_offer/our_policies/privacy) (last updated June 19, 2009).

49. *Id.*

50. *See infra* Part III.B.1.

of genetic and environmental contributions to human traits, as well as to improve medical professionals' ability to diagnose, treat, and prevent illness.<sup>51</sup> The 1000 Genomes Project is an international research consortium formed "to create the most detailed and medically useful picture to date of human genetic variation."<sup>52</sup> The project's goal is to sequence the genomes of approximately 1200 people worldwide and to make that data "swiftly available to the worldwide scientific community through freely accessible public databases."<sup>53</sup> Similarly, the mission of Harvard School of Medicine's Personal Genome Project ("PGP") is to develop personal genomics technology and practices that "yield identifiable and improvable benefits at manageable levels of risk."<sup>54</sup> It is currently recruiting almost 100,000 volunteers to share their personal and genetic information.<sup>55</sup>

### III. GENETIC INFORMATION PRIVACY IN ONLINE RESEARCH COMMUNITIES

Sharing genetic information—and sharing a lot of it—has become very easy very quickly. Technological advances continue to improve the speed and accuracy of DNA sequencing, and scientific research continues to increase our understanding of what those sequences mean as predictors of health, disease, or response to pharmaceuticals. Further, the Internet allows for convenient, rapid dissemination of all of that information: the reports about improved sequencing techniques, the announcements of the latest medical breakthroughs, and uploads of the sequence data itself. For-profit companies and non-profit consortiums are already taking advantage of the Internet as a venue for genetic research studies and as a source of research subjects. But all of this is happening at least one step ahead of legislators. This section explores the extent to which genetic information is protected by law, along with how online-based researchers protect the genetic information of their subjects.

---

51. See, e.g., PERSONAL GENOME PROJECT, <http://www.personalgenomes.org> (last visited Apr. 3, 2011).

52. Press Release, 1000 Genomes Project, International Consortium Announces the 1000 Genomes Project 1 (Jan. 22, 2008), <http://www.1000genomes.org/sites/1000genomes.org/files/docs/1000genomes-newsrelease.pdf>.

53. *Id.*

54. *Mission*, PERSONAL GENOME PROJECT, <http://www.personalgenomes.org/mission.html> (last visited Apr. 5, 2011).

55. PERSONAL GENOME PROJECT, *supra* note 51.

### A. Relevant Legislation

Genetic information is unique compared to other types of health information because it “can reveal information about an individual’s current family members and future offspring” including “predispositions and personal characteristics” even when those predispositions and characteristics are not readily apparent from a person’s appearance or current health status.<sup>56</sup> Additionally, genetic information is “remarkably identifiable.”<sup>57</sup> In the United States, federal and state legislation provides some protection against misuse of this information.

#### 1. The Genetic Information Nondiscrimination Act of 2008

Reports of discrimination based on genetic information began as early as 1991.<sup>58</sup> Federal legislation, including the Americans with Disabilities Act, Title VII of the Civil Rights Act of 1964, and the Health Insurance Portability and Accountability Act, did not directly address genetic information and protection under these acts remained uncertain, and at best, limited.<sup>59</sup> States attempted to supplement federal legislation,<sup>60</sup> but the resulting patchwork of laws provided “inadequate” protection from discrimination.<sup>61</sup>

The Genetic Information Nondiscrimination Act (“GINA”) was passed in 2008 to provide “national and uniform” protection against genetic discrimination.<sup>62</sup> It prohibits employers from discriminating against job applicants or current employees based on their genetic information.<sup>63</sup> It also amended the Employee Retirement Income Security Act of 1974 (“ERISA”),<sup>64</sup> the Public Health Service Act (“PHS”),<sup>65</sup> the Internal Revenue Code of 1986 (relating to group health

56. Jeffrey P. Braff et al., Am. Health Lawyers Ass’n’s Advisory Council on Racial & Ethnic Diversity, *Patient-Tailored Medicine, Part Two: Personalized Medicine and the Legal Landscape*, J. HEALTH & LIFE SCI. L., Jan. 2009, at 1, 37 (citing James G. Hodge, Jr., *Ethical Issues Concerning Genetic Testing and Screening in Public Health*, 125C AM J. MED. GENETICS 66, 69 (2004)).

57. *Id.*

58. Morse Hyun-Myung Tan, *Advancing Civil Rights, The Next Generation: The Genetic Information Nondiscrimination Act of 2008 and Beyond*, 19 HEALTH MATRIX 63, 73-77 (2009) (reviewing instances of genetic discrimination).

59. See Daniel Schlein, *New Frontiers for Genetic Privacy Law: The Genetic Information Nondiscrimination Act of 2008*, 19 GEO. MASON U. C.R. L.J. 311, 318-40 (2009).

60. See *id.* at 347-50; Tan, *supra* note 58, at 89-93.

61. See Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881, § 2 (2008).

62. *Id.*

63. 42 U.S.C.A. §§ 2000ff to ff-11 (West 2010).

64. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 101, 122 Stat. 881 (2008) (to be codified in scattered sections of 29 U.S.C.).

65. *Id.* § 102 (to be codified at 42 U.S.C. §§ 300gg to gg-53, amended by Patient

insurance),<sup>66</sup> and Title XVIII of the Social Security Act (relating to Medicare supplemental insurance)<sup>67</sup> to uniformly prohibit issuers of both individual and group health insurance plans from using genetic information for underwriting purposes, both when issuing a policy and when setting its price.<sup>68</sup>

Although GINA fills in many gaps left by the previous patchwork of legislation and common law, it is not comprehensive. It does not protect information about the actual manifestation of a disease or disorder.<sup>69</sup> GINA also does not cover “spheres of life” outside of employment and insurance.<sup>70</sup> And within the context of insurance, it covers only health insurance; disability, long-term care, and life insurance are not included. Although insurers cannot “request, require, or purchase” genetic information, collecting that information “incidental” to acquiring other allowable information is permitted.<sup>71</sup> Furthermore, GINA says nothing about genetic discrimination by financial service providers or in social contexts. Importantly, GINA does not protect information in the public domain, such as information on the Internet.

## 2. State Laws

GINA preempts state laws only to the extent of mandating minimum standards;<sup>72</sup> states are free to enact legislation with stricter genetic information protections. Although GINA’s insurance provision is limited to health insurance, 17 states currently have laws that cover other types of insurance.<sup>73</sup> Fourteen states restrict genetic information discrimination in life insurance, 15 states do so for disability insurance, and nine do so for long-term care insurance.<sup>74</sup>

---

Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010)).

66. *Id.* § 103 (to be codified in scattered sections of 26 U.S.C., amended by Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010)).

67. *Id.* § 104 (to be codified at 42 U.S.C. § 1395ss, amended by Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010)).

68. *Id.* §§ 101-05 (to be codified in scattered sections of 26 U.S.C., 29 U.S.C., 42 U.S.C.).

69. Amy L. McGuire & Mary Anderlik Majumder, *Two Cheers for GINA?*, 1 GENOME MED. 6.1, 6.2 (2009).

70. Patrick Taylor, *When Consent Gets in the Way*, 456 NATURE 32, 33 (2008).

71. *E.g.*, 29 U.S.C.A. § 1182 (West 2010); 42 U.S.C.A. § 300gg-1 (West 2010).

72. Tan, *supra* note 58, at 103.

73. *Genetics and Life, Disability and Long-Term Care Insurance*, NAT’L CONFERENCE OF STATE LEGISLATURES, <http://www.ncsl.org/IssuesResearch/Health/GeneticNondiscriminationLawsinLifeDisability/t/abid/14283/Default.aspx> (last updated Jan. 28, 2008).

74. *Id.*

## B. Privacy Policies, Terms of Service, and Informed Consent

DTC-GTCs and non-profit research consortiums acknowledge genetic information privacy risks to varying degrees. Given the online nature of these groups, traditional signed consent forms have been replaced by click-through agreements, and traditional face-to-face conversations with medical professionals have been replaced by privacy policies and terms of service documents posted on websites. This section examines how online-based genetic research groups are—or are not—using these surrogate documents to adequately inform research participants of potential risks inherent in their population.

### 1. Direct-to-Consumer Genetic Testing Companies

23andMe uses a lengthy Privacy Statement and Terms of Service agreement to address the types of information the company collects, how the company uses that information, and how they protect it.<sup>75</sup> Personal Information (“information that can be used to identify [a user] either alone or in combination with other information”) is sub-categorized in part as Registration Information (name, email address, etc. used to create an account or purchase services), Genetic Information (such as the data generated by processing a user’s DNA sample), and Self-Reported Information (such as a user’s survey responses).<sup>76</sup> Aggregated Genetic and Self-Reported Information, which has been “stripped of Registration Information and combined with data from . . . other users . . . to minimize the possibility of exposing individual-level information,”<sup>77</sup> from *all* users may be shared with both non-profit and commercial third parties.<sup>78</sup> If a user chooses to participate in 23andWe Research—which the company encourages its users to do<sup>79</sup>—then that user’s information, in aggregated form, may also be disclosed to third parties for the purpose of publication in scientific journals.<sup>80</sup> In other words, the only difference in information disclosure between 23andWe participation and non-participation is that personal information of the former group, but not the latter, may be published in scientific journals.

---

75. *Privacy Statement*, 23ANDME, <https://www.23andme.com/about/privacy> (last updated June 24, 2010); *Terms of Service*, 23ANDME, <https://www.23andme.com/about/tos> (last visited Apr. 5, 2011).

76. *Terms of Service*, *supra* note 75, § 1.

77. *Id.*

78. *Privacy Statement*, *supra* note 75.

79. *Consent Document*, *supra* note 43.

80. *Privacy Statement*, *supra* note 75.

23andMe requires informed consent in order to participate in 23andWe,<sup>81</sup> and the company suggests that its Consent Document is “based upon an IRB-approved consent document.”<sup>82</sup> 23andMe also requires informed consent for the company to share Registration Information with third-party research partners.<sup>83</sup> The company does not mention whether third parties with whom it shares information will be required to protect the confidentiality of that information or to refrain from attempts to reidentify individual contributors.<sup>84</sup>

23andMe has posted information about GINA on its website and acknowledges some, but not all, of the gaps in GINA’s protection.<sup>85</sup> In general, however, the company does warn consumers that sharing genetic data can lead to unintended consequences, such as a third party discovering additional information about a user, or future scientific advances causing a revelation that could not have been predicted.<sup>86</sup>

Despite not having research arms as apparent as 23andMe’s, other DTC-GTCs are no less likely to use their customers’ genetic information for research purposes.<sup>87</sup> For example, in its Privacy Policy, Navigenics states that it “believes in . . . helping further scientific and medical research.”<sup>88</sup> In promotion of that belief, it may use its customers’ Genetic Data (i.e. the DNA genotyping results) linked to their Phenotype Information (defined to include, for example, gender, height, weight, ethnicity, and ancestry, as well as health conditions and diseases of the user and the user’s family members) to “[d]iscover or validate associations between certain genetic variations and certain health conditions or traits.”<sup>89</sup> The company may also publish its findings “without disclosing [a user’s] Genetic Data in a quantity sufficient to uniquely identify [a user].”<sup>90</sup> Navigenics’s Informed Consent document does state that Genetic Data and Phenotype Information will be used by the company

81. *Consent Document*, *supra* note 43.

82. *Terms of Service*, *supra* note 75, § 5. It is unclear whether the Terms of Service is referring to the actual Consent Document, and it is also unclear from where the “IRB-approved” document that 23andMe based its own document upon came.

83. *Privacy Statement*, *supra* note 75.

84. *See infra* Part IV.A.1.

85. “GINA does not cover life or disability insurance providers.” *What is Gina?*, 23ANDME, <https://www.23andme.com/you/faqwin/gina> (last visited Apr. 12, 2011).

86. *Considerations*, 23ANDME, <https://www.23andme.com/more/considerations> (last visited Feb. 24, 2011). *See also Consent Document*, *supra* note 43.

87. *Cf.* Heidi C. Howard et al., *Blurring Lines*, 11 EMBO REPORTS 579, 579 (2010) (reporting that DTC genetic testing companies vary in their candidness about and clarity on use of customers’ genetic information for research purposes).

88. *Privacy Policy*, *supra* note 48.

89. *Id.*

90. *Id.* Presumably Navigenics is aware of how little genetic data is required to identify an individual. *See* Lin et al., *infra* note 129; *see also infra* Part IV.A.1.

for internal research,<sup>91</sup> but it does not give any specifics about the potential subject areas or scope of that research, nor does it state whether that research has been approved by an independent authority, such as an IRB.<sup>92</sup>

Navigenics also gives its customers opportunities to share their Genetic Data and Phenotype Information with not-for-profit third-party organizations who conduct genetic or medical research.<sup>93</sup> These organizations may also publish their study results and “deposit such [Genetic Data and Phenotype Information] . . . into public data repositories or otherwise make them publicly available.”<sup>94</sup> It is unclear whether this is an opt-in or opt-out system.

deCODEme, another DTC-GTC, may invite its customers “to participate in studies or other research activities,”<sup>95</sup> which suggests that participation is voluntary. However, both the company’s Privacy Policy and Service Agreement also state that deCODEme may use its customers’ information to gather statistical aggregate data,<sup>96</sup> which suggests at least minimal automatic use for internal research purposes. Additionally, that data may include “associating genetic variants with any of the self-reported user attributes,”<sup>97</sup> which further suggests that the company is linking Genetic Information with Self-Reported Information (as 23andMe would describe it). Because the Service Agreement (which users must agree to before their DNA samples are analyzed) doubles as deCODEme’s “informed” consent document,<sup>98</sup> it is unclear whether the company would seek additional consent for participation in the research studies that it invites its users to join. The company’s website also does not mention whether deCODEme has sought independent approval for use of its data in research studies.

Currently, fellow DTC-GTCs Lumigenix and Pathway Genomics do not appear to be conducting any in-house research, but both

91. *Informed Consent, Health Compass*, NAVIGENICS, [http://www.navigenics.com/visitor/what\\_we\\_offer/our\\_policies/informed\\_consent/health\\_compass](http://www.navigenics.com/visitor/what_we_offer/our_policies/informed_consent/health_compass) (last visited Feb. 24, 2011).

92. Seeking independent approval of a study plan would be voluntary because private DTC-GTCs such as Navigenics are currently not obligated to obtain permission for research studies. See *infra* Part V.B.2.

93. *Privacy Policy*, *supra* note 48.

94. *Id.*

95. *Terms of Use*, DECODEME, <http://www.decodeme.com/terms-of-use> (last updated June 2, 2007).

96. *Privacy Policy*, DECODEME, <http://www.decodeme.com/privacy-policy> (last updated Nov. 12, 2007); *Service Agreement*, DECODEME, <http://www.decodeme.com/service-agreement> (last updated Nov. 30, 2009).

97. *Id.*

98. The full name of the document is “deCODEme Genetic Scan Service Agreement and Informed Consent.” *Service Agreement*, *supra* note 96.

companies may collaborate with other organizations who conduct research.<sup>99</sup> Not only do both companies pledge to obtain their customers' express consent before sharing any data with collaborators, they will also require that collaborators obtain study permission from an IRB.<sup>100</sup>

## 2. Non-Profit Research Consortiums

The privacy risks associated with participation in the 1000 Genomes Project are seemingly low because the researchers are not collecting any personally identifying or medical information from subjects.<sup>101</sup> Most of the genome sequences will come from DNA previously submitted to another project for which no personally identifying or medical information was collected either.<sup>102</sup>

In complete contrast, privacy and confidentiality for subjects in the Personal Genome Project will be almost non-existent.<sup>103</sup> Because one of the PGP's goals is to explore research and commercial uses of human genetic data linked to trait information,<sup>104</sup> almost all information submitted by a participant, including physical trait and medical information, and even photographs, will be posted on the PGP's public website and database along with genetic information.<sup>105</sup>

To help ensure that study participants understand the implications of their involvement, interested individuals must first submit to a rigorous IRB-approved pre-enrollment process that begins with an eligibility questionnaire and an entrance exam.<sup>106</sup> The latter assesses "comprehension of concepts . . . includ[ing] . . . potential risks of participating, project protocols, and basic genetics";<sup>107</sup> a passing score of no less than 100 percent

99. *Privacy Policy*, LUMIGENIX, <http://www.lumigenix.com/privacy> (last updated Nov. 10, 2010); *Privacy Statement*, PATHWAY GENOMICS, <https://www.pathway.com/about-us/privacy-policy> (last visited Apr. 12, 2011).

100. *Supra* note 99.

101. Press Release, *supra* note 52, at 2.

102. *Id.* at 4 (noting that samples collected, without any medical or identifying information, for the HapMap project will be used for much of the 1000 Genomes Project). *But see infra* Part IV.A.1 (discussing reidentifiability of an individual anonymous contributor to a pool of thousands of DNA samples, such as that compiled by the HapMap project).

103. PERSONAL GENOME PROJECT, CONSENT FORM: PERSONAL GENOME PROJECT § X:10.1 (2010), *available at* [http://www.personalgenomes.org/consent/PGP\\_Consent\\_Approved03312010.pdf](http://www.personalgenomes.org/consent/PGP_Consent_Approved03312010.pdf) [hereinafter FULL CONSENT] (explaining that PGP will not keep data in a confidential or anonymous fashion, nor will it require third parties who access the data to do so).

104. PERSONAL GENOME PROJECT, CONSENT FORM: ELIGIBILITY SCREENING FOR THE PERSONAL GENOME PROJECT § I (2010), *available at* [http://www.personalgenomes.org/consent/PGP\\_MiniConsent\\_Approved03312010.pdf](http://www.personalgenomes.org/consent/PGP_MiniConsent_Approved03312010.pdf) [hereinafter MINI CONSENT].

105. FULL CONSENT, *supra* note 103, §§ IV:4.1, V:5.1, V:5.5.

106. MINI CONSENT, *supra* note 104, § IV:4.1-.2.

107. *How It Works*, PERSONAL GENOME PROJECT,

correct is required.<sup>108</sup> If an applicant is deemed eligible to continue, the next pre-enrollment steps include submitting baseline trait data<sup>109</sup> and verifying identity.<sup>110</sup> After the PGP enrolls an individual, the baseline trait data is published on the PGP's public website and database, and the enrollee submits tissue samples.<sup>111</sup> Those tissue samples are used for DNA analysis, which in turn is used to generate a Preliminary Research Report that should help participants decide whether or not to release their genetic data to the public website and database<sup>112</sup> where it will be associated with the previously-submitted baseline trait data.<sup>113</sup> Once released, neither the participant nor the PGP can control who has access to, makes copies of, or otherwise uses the information.<sup>114</sup>

This ready accessibility suggests a myriad of worrisome scenarios limited only by imagination. According to the PGP, "anyone with sufficient knowledge and resources" could use the online data to truthfully claim that a participant is, for example, predisposed to a disease or related to criminals.<sup>115</sup> If someone altered and republished the data the same claims of disease predisposition or criminal relationships could be falsely made.<sup>116</sup> Someone could even "make synthetic DNA and plant it at a crime scene,"<sup>117</sup> thus implicating an innocent person in a crime. Additionally, although the information will not intentionally become part of a participant's medical record, the information could be identified with a particular individual and added to that person's record,<sup>118</sup> possibly affecting access to health insurance despite GINA. Further, GINA permits employers to acquire genetic information from the public domain, which would include the PGP's public website and database.<sup>119</sup>

---

<http://www.personalgenomes.org/howitworks.html> (last visited Feb. 24, 2011). This type of informed consent, in which researchers openly admit that subjects' privacy and anonymity cannot be guaranteed, and subjects then consent to the possibility of complete public disclosure of their information, is called "open consent." Jeantine E. Lunshof et al., *From Genetic Privacy to Open Consent*, 9 NATURE REV. GENETICS 406, 409 (2008).

108. MINI CONSENT, *supra* note 104, § IV:4.2.

109. Baseline trait data may include "date of birth, medications, allergies, vaccines, personal medical history, race/ethnicity/ancestry, and vital signs" as well as family medical history and a facial photograph. FULL CONSENT, *supra* note 103, § IV:4.1.

110. *Id.* § IV.

111. FULL CONSENT, *supra* note 103, § V:5.1-.3. An enrollee may choose not to publish her baseline trait data, but that may make her ineligible to participate in other aspects of the study. *Id.* § V:5.1(b).

112. *Id.* § V:5.4-.5.

113. *Id.* § V:5.5(c).

114. *Id.* § VII:7.1(c).

115. *Id.* § VII:7.1(a)(iii).

116. *Id.*

117. *Id.*

118. *Id.* § X:10.4.

119. *See, e.g.*, 42 U.S.C.A. § 2000ff-1(b)(4) (West 2010).

#### IV. PRIVACY VERSUS PUBLIC BENEFIT

We have a lot to gain, and a lot to lose, from genetic research. Medical and scientific advancements depend on information about how genes influence traits and diseases. Yet mere collection of DNA for the research that provides that information can compromise an individual's privacy and anonymity. This section highlights some of the competing values and concerns that shape the debate over how best to balance the benefits and risks of online-based genetic research.

##### *A. Privacy Concerns*

An individual who chooses to participate in an online-based research study may not be aware of the risks to his privacy, especially if the researcher does not fully inform him of these risks. These risks include loss of anonymity (even if the researcher "promises" confidentiality or anonymity) and genetic discrimination (despite GINA). This section highlights some of the privacy risks associated with participation in an online-based genetic research study.

##### 1. Reidentification: The Loss of Anonymity

One's DNA sequence or carrier status for a particular disease-related gene is undoubtedly information that most people would want to keep private or at least limit the dissemination of. When other types of private information, such as name, social security number, or address, are collected, they are usually anonymized before being shared or released. Typically this means the identifying information is deleted from the rest of the data. For decades this has led to a "robust anonymization assumption,"<sup>120</sup> the belief that by removing certain pieces of information from data the individual to whom the data corresponds would remain anonymous. Unfortunately, recent studies have shown the failure of that assumption. For example, in the mid-1990s a Massachusetts government agency that purchased health insurance for state employees, the Group Insurance Commission ("GIC"), made its patient records available to researchers.<sup>121</sup> First, of course, GIC removed "explicit identifiers" such as name, address, and social security number.<sup>122</sup> Still, one industrious researcher was able to use birth date, sex, and ZIP code to identify the governor of Massachusetts (who had assured the public that patients' information would remain private) from within the

---

120. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 (2010).

121. *Id.* at 1719.

122. *Id.*

“deidentified” database of patient records.<sup>123</sup> This matching of seemingly anonymous information to the specific individual from whom the information was derived is known as *reidentification*.

Similarly, a 2008 study shocked the genetic research community by proving it was possible to identify a single individual’s DNA contribution from a pool of thousands of DNA samples.<sup>124</sup> One commentator explained that “[b]ecause the pool consists of DNA from so many people, the assumption ha[d] been that it would be impossible to identify any one individual’s DNA.”<sup>125</sup> The National Institutes of Health (“NIH”) had been so “confident in the anonymity of pooled genetic data that it recommended it be made public for all researchers to use.”<sup>126</sup> After the 2008 study was published, the NIH and other similar research institutions removed some genetic data from their publicly accessible websites,<sup>127</sup> stating that “[t]he greatest concern is that identifying an individual this way could reveal sensitive health information.”<sup>128</sup>

Before reidentification concerns surfaced, a 2004 computational study had already determined that as few as 30 SNPs will uniquely identify a single person.<sup>129</sup> This is troubling because up to a million SNPs are usually examined in DTC genetic testing.<sup>130</sup> Thus, someone with access to both individual and public genetic data could identify the individual using just a small set of SNPs.<sup>131</sup>

What this means for participants in DTC genetic testing research studies, as well as for subjects in non-profit research consortium studies, is that there is no safety in numbers. Even though hundreds or thousands of individuals’ genetic information may be pooled for so-called genome-wide association studies, a single person could be pinpointed within that pool. To the extent that these research projects *offer* privacy or anonymity, they can no longer *guarantee* either.

Any sharing of genetic data, even deidentified data, with fellow researchers or third parties (as DTC-GTCs acknowledge they may do, and non-profit research consortiums readily do) opens up the possibility

123. *Id.* at 1719-20.

124. Nils Homer et al., *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays*, 4 PLOS GENETICS 1, 7 (2008), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2516199/pdf/pgen.1000167.pdf>.

125. Jennifer Couzin, *Whole-Genome Data Not Anonymous, Challenging Assumptions*, 321 SCIENCE 1278, 1278 (2008).

126. *Id.*

127. *Id.*

128. *Id.*

129. Zhen Lin et al., *Genomic Research and Human Subject Privacy*, 305 SCIENCE 183, 183 (2004).

130. *How Does 23andMe Genotype My DNA?*, *supra* note 41.

131. Lin et al., *supra* note 129.

that someone—for good or for ill—will “reverse engineer” the data and defeat intended privacy protections.

## 2. Informed Consent and Autonomy

Participants in traditional clinical trials usually meet with a health care provider who can explain informed consent forms and answer related questions. In contrast, research participants who enroll online do not interact personally with anyone, let alone a medical professional. If a potential subject has a question, it is more likely to be answered by email than by telephone, certainly not in person, and not necessarily by a medical professional. This physical and emotional separation between parties can create a false sense of security, and the casualness of the online environment in general can create the impression that joining a genetic study is trivial. After all, enrollment takes just a few clicks of a mouse. Computer users are already accustomed to click-through agreements, and there is no reason to believe that they treat informed consent forms any differently than software use agreements.<sup>132</sup> For enrollees who do actually read the consent forms, concerns remain that they do not comprehend the content.<sup>133</sup>

An individual's choice to participate in a research study or otherwise share his or her genetic information should be respected. However, one of the unique aspects of genetic information—that parts of it are common to one's blood relatives—implicates choice and autonomy for family members who do not want to share their genetic information, and perhaps do not want to know any secrets that their or their relatives' DNA sequences might reveal.<sup>134</sup> For example, identical twins have identical DNA sequences, so if one twin contributes his genetic

132. Gabrielle Kohlmeier, *The Risky Business of Lifestyle Genetic Testing: Protecting Against Harmful Disclosure of Genetic Information*, UCLA J.L. & TECH., Fall 2007, at 42 n.149.

133. Amy L. McGuire & Richard A. Gibbs, *No Longer De-Identified*, 312 SCIENCE 370, 371 (2006). “As is widely recognized in a medical context, a signature on a consent document does not necessarily indicate . . . understanding.” Katherine Wasson, *Direct-to-Consumer Genomics and Research Ethics: Should a More Robust Informed Consent Process Be Included?*, 9 AM. J. BIOETHICS 56, 57 (2009). Yet lack of comprehension appears to be legally sufficient. Kohlmeier, *supra* note 132, at 40 (citing *Canterbury v. Spence*, 464 F.2d 772 (D.C. Cir. 1972), for the proposition that legal informed consent does not require comprehension).

134. See Amy L. McGuire et al., *Research Ethics and the Challenge of Whole-Genome Sequencing*, 9 NATURE REV. GENETICS 152, 154 (2008) (recommending that “participants . . . include close genetic relatives in decisions about research participation” because “[c]linically relevant . . . information about family members' health risks can be revealed during the course of data analysis”). Cf. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291 (2010) (arguing against the practice of familial searching—the practice of searching for partial matches to crime scene DNA evidence in order to identify potential relatives of the source, who is often the suspected perpetrator—on numerous grounds, including privacy).

information to a research study, his twin essentially does as well, perhaps without consent or even knowledge.

### 3. Genetic Discrimination

Despite the protections that GINA does afford, the Act does not prohibit genetic discrimination based on publicly or commercially available information, such as information on the Internet. Nor do its provisions protect against discrimination by financial service providers, by insurers other than health insurers, or by society as a whole. Although GINA's provisions prohibit an employer from using private genetic data to effect discrimination, concerns remain about the employer who "receive[s] genetic information in legal ways, us[es] that information illegally, and then rationaliz[es] such use on legal grounds."<sup>135</sup> Participation in genetic research studies, especially in those that make their data or findings publicly accessible,<sup>136</sup> raises the likelihood that an employer or service provider will intentionally or unintentionally come to possess that information, which in turn increases the likelihood that discrimination will result.

#### *B. Public Benefit: Promoting, Not Impeding, Genetic Research*

On the other side of the scale from protecting privacy is many researchers' demand for greater access to and easier sharing of genetic as well as other types of information. This demand arises because genetic information is valuable for research purposes when genotype is linked to phenotype, when what your genes say about you is combined with what you (and your doctor) say about you. For example, researchers cannot determine which genes influence Alzheimer's disease if they do not know which subjects are suffering from Alzheimer's disease, and therefore whose DNA to study. And complex human traits and conditions, those influenced by genetic as well as environmental and other factors, can be accurately studied only by combining individuals' genetic information with their personal information, such as that about medical history, diet, and exercise.<sup>137</sup> Furthermore, longitudinal studies (those that track the same

---

135. Tan, *supra* note 58, at 117. Employers can acquire genetic information through new-hire medical examinations, such as drug testing and fitness-for-duty exams, as well as through health claims submitted to employer-sponsored health plans, workers' compensation claims, and requests for sick, family, and medical leave. Joanne L. Husted & Janlori Goldman, *The Genetics Revolution: Conflicts, Challenges and Conundra*, 28 AM. J.L. & MED. 285, 293-94 (2002).

136. This includes at least DTC-GTCs 23andMe and Navigenics, who may publish their results, as well as most non-profit research consortiums. See *supra* Part III.B.

137. John M. Conley et al., *Enabling Responsible Public Genomics*, 20 HEALTH MATRIX 325, 328 (2010).

participants over an extended period of time) require the ability to connect a particular research participant with that person's data in order to see what traits or conditions have changed over time.<sup>138</sup> The need for linked data to advance health care, then, conflicts with concerns about reidentifiability and discrimination that result from ineffective privacy protections.<sup>139</sup>

The Human Genome Project inspired the view that collections of genetic information were "global public goods"<sup>140</sup> such that "all human genomic sequence information . . . should be freely available and in the public domain."<sup>141</sup> This uninhibited sharing of data was considered an "ethical imperative" in order to maximize the data's value and best promote research and development for the benefit of society.<sup>142</sup> Studies such as the PGP follow this open-access model.

Further support for easier access to data comes from scholars who have noted that informed consent requirements obstruct research by decreasing the data pool because not all individuals will consent.<sup>143</sup> The decreased pool leads to biased results because the elderly, illiterate, and those of lower socioeconomic status are less likely to consent,<sup>144</sup> and consent is less likely to be sought from the very ill and very impaired.<sup>145</sup> Those who do participate "represent a self-selected group that could skew research results."<sup>146</sup>

According to some medical professionals, HIPAA's consent requirements have also had a "profoundly negative impact" on research.<sup>147</sup> These requirements include that "patients have to give consent for each use of their data."<sup>148</sup> In practice, this has prevented separate institutions

138. *See id.* at 341.

139. It is worth noting that linking genotypic and phenotypic data does not automatically mean that the individual who supplied that data will be identified, but rather that "the content of the data renders it inherently identifiable." *Id.*

140. Bartha Maria Knoppers, *Consent to "Personal" Genomics and Privacy*, 11 EMBO REP. 416, 417 (2010) (quoting HUGO Ethics Committee, *Statement on Human Genomic Databases of 2002*, 13 EUBIOS J. ASIAN & INT'L BIOETHICS 99 (2003)).

141. *Id.* (quoting HUMAN GENOME ORGANIZATION, PRINCIPLES AGREED AT THE FIRST INTERNATIONAL STRATEGY MEETING ON HUMAN GENOME SEQUENCING (1996)).

142. *Id.* (quoting European Soc'y of Human Genetics, *Data Storage and DNA Banking for Biomedical Research*, 11 EUR. J. HUM. GENETICS 906 (2003)).

143. Julie R. Ingelfinger & Jeffrey M. Drazen, *Registry Research and Medical Privacy*, 350 NEW ENG. J. MED. 1452, 1453 (2004).

144. Taylor, *supra* note 70, at 32.

145. Ingelfinger & Drazen, *supra* note 143.

146. Francis S. Collins & James D. Watson, *Genetic Discrimination: Time to Act*, 302 SCIENCE 745, 745 (2003).

147. Jocelyn Kaiser, *Privacy Rule Creates Bottleneck for U.S. Biomedical Researchers*, 305 SCIENCE 168, 169 (2004) (referring to a survey by the American Association of Medical Colleges).

148. *Id.*

that have already conducted research studies—with patient consent—from pooling their genetic data to look for medical and genetic trends.<sup>149</sup>

Additionally, some commentators have pointed out that SNP data has little predictive value on its own,<sup>150</sup> so we should not rush to prioritize privacy over research progress when dealing with data disclosures. Indeed, genetic determinism—the belief that genes alone determine all of the physical and behavioral characteristics of an individual—is a discredited notion.<sup>151</sup> The vast majority of traits (e.g. height, hair color) and diseases (e.g. cardiovascular disease, colon cancer) arise from a complex mixture of many gene products, environmental factors, and individual choice.<sup>152</sup> If revelation of one’s genetic information does not actually reveal that much, then suppressing its release and use harms medical research more than it helps an individual’s privacy. At the very least, research and privacy must be balanced instead of requiring that “research has to demonstrate that the public interest substantially outweighs privacy protection.”<sup>153</sup>

### C. *Balancing Concerns*

The more information to which researchers have access, and the more complete that information is, the more accurate and reliable their study results are. Ease of communication on the Internet could lead to more study participation by a broader group of people, thereby improving data breadth and the robustness of research conclusions. In turn, this information would contribute to medical and scientific advancements that help the general public. But with that ease of communication comes ease of reidentification, increased opportunities for discrimination, and concerns that participants do not fully appreciate the consequences of a click of a mouse. These potential benefits and harms must be balanced so as to not stifle scientific progress in the preservation of individual privacy, nor sacrifice personal rights for the sake of medical advances.

---

149. *See id.* (reporting that 14 institutions involved in a prostate cancer genetics study could not pool their data to look for cancer susceptibility genes and instead were limited to sharing summaries of their analyses).

150. Barbara Prainsack et al., *Misdirected Precaution*, 456 NATURE 34, 35 (2008).

151. *See, e.g.*, David B. Resnik & Daniel B. Vorhaus, *Genetic Modification and Genetic Determinism*, 1 PHIL. ETHICS & HUMAN. MED. 1, 3-4 (2006), <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1524970/pdf/1747-5341-1-9.pdf>.

152. *See, e.g., id.* at 4.

153. Knoppers, *supra* note 140, at 418.

## V. RECOMMENDATIONS

Unlike the Tuskegee men, direct-to-consumer genetic testing subscribers are not in danger of becoming unwitting participants in a study on untreated syphilis. Likewise, subjects in a non-profit research consortium's genetic study need not fear being intentionally infected with hepatitis, as were the children at Willowbrook. Yet the members of this novel cohort of genetic research participants still deserve respect for their privacy, deference to their autonomy, and protection from discrimination. However, ensuring that these criteria are met should not come at the expense of scientific and technological progress. This final section proposes several approaches to balancing these competing private and public concerns.

### *A. Addressing Reidentifiability*

Ultimately, problems with participation in Internet-based human genetics research studies lie not in the participation itself, but in the unintended consequences of participation. The primary unintended consequence is reidentification—that someone (inside or outside of the research study) will determine not only that a given individual participated, but what the participant's genetic contribution says about that person. If a study organizer could guarantee that his subjects' identities would remain confidential and their genetic data would remain private, the remaining concerns and arguments would be relatively benign. For example, advocates for patients' autonomy might still worry about truly informed consent in the absence of a doctor-patient relationship, or statisticians might bemoan that DTC-GTCs' solicitation of customers as research subjects is skewing the data pool.

Unfortunately, the solution is not as simple as an outright ban on reidentification; because the act of connecting the dots from anonymized data to the corresponding individual cannot itself be detected, a ban would be ineffective.<sup>154</sup> Even if it could be detected and prevented, technology will always leave enforcers one step behind reidentifiers: “[I]n the arms race between . . . anonymization and reidentification, the reidentifiers hold the permanent upper hand.”<sup>155</sup>

One proposal for addressing reidentification suggests restricting the flow of (in the instant case, genetic) information such that disclosures

154. Ohm, *supra* note 120, at 1758.

155. *Id.* at 1752. See also Bradley Malin & Latanya Sweeney, *How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity Protection Systems*, 37 J. BIOMEDICAL INFORMATICS 179, 191 (2003) (“[W]e are developing more robust . . . re-identification algorithms.”).

occur only to the extent that the benefits outweigh the costs to privacy.<sup>156</sup> In the medical research community, regulators could build upon intrinsic “human networks of trust” that already exist among professionals.<sup>157</sup> This is a great suggestion for data generated from traditional human subject research projects set at a hospital, university, or other collegial institution, but it is unlikely to be effective in an arms-length commercial model such as 23andMe’s or Navigenics’s collaborations with outside researchers. Also, it is inapplicable to an endeavor such as the Personal Genome Project, because one of the PGP’s goals is to determine the results, both positive and negative, of free and unrestricted public sharing of genetic information. If reidentification is one of those results, the investigators would certainly want to know.

Given that the real concerns from study participation stem from privacy and discrimination issues attendant to reidentification, all of the suggested reforms below must be considered in light of, or as attempts to mitigate, the reidentifiability risk.

### *B. Legislative Reform*

Current federal legislation does not go far enough to protect the privacy of participants in online-based genetic research studies. Some reforms should be made, but others may not protect participants enough to justify the negative impact they could have on research. This section proposes and analyzes some possible legislative amendments.

#### 1. Expansion of the Genetic Information Nondiscrimination Act

The protections afforded by GINA should be expanded to cover all genetic information, including that found in the public domain, such as on the Internet, and information derived via reidentification. Specifically, and at a minimum, GINA should provide protection against the use of genetic information that has been shared in support of a valid research project.

Expanding GINA in this way will help ameliorate some of the effects of reidentification, as well as promote personal autonomy and consumer choice (i.e. individuals still get to make decisions about accessing, or not accessing, their genetic information) while simultaneously boosting participation in research due to the (perceived) protection from discrimination based on one’s genetic information.

---

156. See Ohm, *supra* note 120, at 1768-69.

157. *Id.* at 1770.

The weakness in this suggestion, however, is that discrimination is hard to prove, and appealing to insurance companies' and employers to "not peek" when the information is readily accessible is unlikely to be successful. Additionally, expanding GINA does nothing to address informed consent and may even mislead potential research participants into thinking that they are completely protected by the law.

However, despite the fact that reforming GINA will not prevent reidentification or completely eliminate genetic-based discrimination, the proposed changes should still be enacted because they fill in legislative gaps from which abuse by an employer or insurer could arise.

## 2. Revising the Common Rule

Currently, the Common Rule requires Institutional Review Board-approval only for institutions that receive federal funds or who are otherwise federally regulated. Research carried out by a private company that does not produce a pharmaceutical or other regulated product is exempt from the IRB requirements. Therefore, a private Internet-based company such as 23andMe, which offers only genetic sequencing and analysis services, is not required to seek IRB approval for the research projects its research arm, 23andWe, undertakes.

The Common Rule could be expanded to include research projects implemented by companies currently outside of the Rule's reach. Then, like investigators at large academic universities or scientists at pharmaceutical companies, researchers at companies like 23andMe would have to draft research proposals and seek IRB approval before commencing genetic information studies. Their studies would be evaluated to ensure that the risks to the subjects are both minimized and reasonable in relation to the anticipated benefits. Selection of subjects would need to be equitable and informed consent would have to be obtained. The consent form would need to include a description of risks to the subject, an identification of benefits to the subject or to others, and a statement that participation is voluntary and the subject may withdraw at any time. A statement describing the extent of confidentiality of records identifying the subject will also have to be included, as the existence of adequate provisions for protecting the privacy of subjects and maintaining confidentiality of data is one of the criteria considered by IRBs when they evaluate proposals.

This is likely to be a politically unpopular approach, as it would greatly expand the scope of oversight to currently unregulated private companies—those that receive no federal funding and do not produce a good regulated by the federal government. The tests offered by DTC-GTCs (and hence the vehicle by which the public participates in one of

their research studies) are currently not regulated by the FDA. Several scholars have argued for the tests to fall under the auspices of the FDA because a similar (if not as comprehensive) test ordered by one's personal physician *does* require FDA regulation and approval.<sup>158</sup> Additionally, or alternatively, DTC genetic tests could be regulated by the Clinical Laboratory Improvement Amendment of 1988 ("CLIA").<sup>159</sup>

Changes to the regulatory scheme do appear to be on the horizon,<sup>160</sup> but even if DTC-GTCs' tests become subject to FDA regulation, and if the companies are required to seek IRB approval for their research studies,<sup>161</sup> what change will be effected? Historically, the "harm" that IRB committees look for, and try to ensure that investigators minimize, is physical harm.<sup>162</sup> DTC research participants face no physical harm or intrusion; they spit into a tube. The psychological and emotional harm that could come from learning something devastating about one's genetic profile—such as carrying the gene for the aggressive and fatal Huntington's disease—is no more extensive than if the subject opted only for the testing service and chose not to participate in the study.

158. Scholars have been concerned that DTC genetic testing services are not safe or efficacious, have not been clinically or analytically validated, and even have suspect clinical utility. See, e.g., Lauren B. Solberg, Note, *Over the Counter But Under the Radar: Direct-to-Consumer Genetics Tests and FDA Regulation of Medical Devices*, 11 VAND. J. ENT. & TECH. L. 711, 720, 722 (2009). More problematic is that no federal agency is responsible for ensuring that the tests meet any particular quality standards. See, e.g., Jennifer A. Gniady, Note, *Regulating Direct-to-Consumer Genetic Testing: Protecting the Consumer Without Quashing a Medical Revolution*, 76 FORDHAM L. REV. 2429, 2436-37 (2008). The Federal Trade Commission can regulate advertisement of DTC tests, but critics contend the Commission has not taken action against advertisements that may be false or misleading. Solberg, *supra*, at 722. If regulated, DTC genetic tests would likely fall under the guise of medical devices, which the Food and Drug Administration regulates. See Gail H. Javitt, *In Search of a Coherent Framework: Options for FDA Oversight of Genetic Tests*, 62 FOOD & DRUG L.J. 617, 618-19 (2007).

159. CLIA governs all laboratories that perform tests designed to provide information about a person's health. Specifically, it aims to regulate protocols, reagents, quality control procedures and even the qualifications of laboratory personnel. Although CLIA governs many of the tangible aspects of genetic testing, it does not ensure any specific standards for accuracy, reliability, or clinical validity. Gniady, *supra* note 158, at 2440; Douglas A. Grimm, *FDA, CLIA, or a "Reasonable Combination of Both": Toward Increased Regulatory Oversight of Genetic Testing*, 41 U.S.F. L. REV. 107, 121 (2006).

160. Dan Vorhaus, *Update: FDA Taking Another (Public) Look at DTC Genetic Tests*, GENOMICS L. REP. (Feb. 8, 2011), <http://www.genomicslawreport.com/index.php/tag/dtc> (reporting that the FDA announced a public meeting, set for March 8, 2011, to discuss DTC genetic tests).

161. This could occur as a direct consequence of FDA regulation or via expansion of the Common Rule.

162. See, e.g., 45 C.F.R. § 46.102(i) (2010) (defining minimal risk—which IRBs seek to achieve—as "mean[ing] that the probability and magnitude of harm . . . anticipated in the research [is] not greater . . . than [that] ordinarily encountered in daily life or during . . . routine physical or psychological examinations").

(Because DTC-GTCs recruit study participants via their existing consumer pool, all potential consequences of study participation must be compared to a baseline of receiving only the genetic testing service, rather than by using “no genetic testing” as a baseline and comparing it to participation in a study that includes discovering genetic information about oneself.<sup>163</sup>) Only under a much broader conception of *harm* might research proposals by DTC-GTCs be denied by IRBs based on “unjustifiable harm” grounds. That is, to the list of possible adverse consequences from participating in a research study, IRBs would have to add genetic discrimination and other social harms,<sup>164</sup> especially those attendant to reidentification. However, those harms are “difficult to forecast” and the “most significant risks . . . may presently be unknown.”<sup>165</sup> Ultimately, then, the Common Rule’s “limited conception of risk leaves it ill-equipped to protect human subjects”<sup>166</sup> in DTC-based research.

Proper informed consent is also an important criterion for gaining IRB approval. 23andMe’s online consent form already meets the requirements for identifying risk to the subject (although it could be beefed up<sup>167</sup>) and the benefits to the participant or others.<sup>168</sup> The consent form also includes the requisite statement that participation is voluntary and the subject may withdraw at any time.<sup>169</sup> However, this is qualified by acknowledging that it takes time to withdraw, and participants’ genetic information that has already been used for research purposes cannot be withdrawn.<sup>170</sup>

The Common Rule’s IRB provision already applies to academic or otherwise publicly-funded research consortiums, except when data is collected from the public domain or when the data is from subjects that cannot be identified. We have seen the fallacy of the claim that subjects “cannot” be identified, so the Rule could be amended to eliminate these (the public domain and de-identified information) exceptions. However, if follow-on investigators want to analyze existing data that was previously collected for a different purpose, these proposed amendments would prohibit that use because the original data contributor (the human

---

163. *But see 23andMe Parkinson’s Community: Strength in Numbers* and *23andMe Sarcoma Community: A Patient-Driven Revolution in Sarcoma Research*, *supra* note 46 (offering genetic testing and research enrollment for free—compared to at least \$199 for the standard testing kit—for Parkinson’s disease and sarcoma patients, which could be considered coercive).

164. *See* Conley et al., *supra* note 137, at 363.

165. *Id.* at 363–64.

166. *Id.* at 364.

167. *See infra* Part V.D.

168. *Consent Document*, *supra* note 43.

169. *Id.*

170. *Id.*

subject) most likely did not consent to the use of his information in a second study.<sup>171</sup> The follow-on investigator would then have to plan and execute her own study, which could be cost-prohibitive for academic researchers already struggling for research funding. Additionally, even if cost were not a factor, increasing the number of studies also increases the amount of data collected, which thereby increases the chances for breaches of privacy and confidentiality of that data, and that is certainly not a beneficial solution.

Overall, these changes to the Common Rule could restrict research without enough counterbalancing privacy protections to justify the stifling effects. Having to seek research approval from an IRB would force DTC-GTCs to create comprehensive research proposals and informed consent documents, and if the IRBs, for their part, started considering reidentification and its consequences as potential harms, the resulting documents could be quite robust. Yet informed consent procedures are already known to inhibit research.<sup>172</sup> Furthermore, the amendments would do nothing to prevent reidentification, and could address it only if and to the extent that IRBs weighed it as a harm. Finally, the proposed changes also would not address or attempt to prevent genetic discrimination.

### *C. Protective Approaches*

Other approaches to safeguarding genetic privacy, while still promoting research, attempt to add an additional layer of protection either between a subject and those who work with the subject's genetic information (stewardships) or between a subject and those who might try to force revelation of a subject's identity (Certificates of Confidentiality). These approaches are explored in turn below.

#### 1. Stewardships

As mentioned earlier, "the utility and privacy of data are intrinsically connected"<sup>173</sup> such that genetic data must be linked to some personal information in order to benefit research. Researchers often use codes to keep a subject linked (keyed) to his or her data (i.e. genetic information) without employing a ready identifier such as the subject's name. The goal of these systems is to maintain privacy without completely losing the importance and value of linked information.

---

171. HIPPA creates similar problems. *See supra* text accompanying notes 147-149.

172. *See supra* Part IV.B.

173. Ohm, *supra* note 120, at 1705.

Some writers have suggested that independent third parties should hold the keys.<sup>174</sup> These stewards of the identifying linkages would not only hold the keys, but “turn” them, using them to “run queries that have passed independent ethical scrutiny.”<sup>175</sup> Although this approach keeps any individual researcher or group of researchers (e.g. sample collectors, DNA sequencers, data analyzers) from knowing “too much,” it is vulnerable to security breaches. These breaches may include “misconduct by the person who retains the key . . . , theft of the key by hackers, and the loss of laptops or other storage devices that contain the keys.”<sup>176</sup>

More importantly, stewardships do nothing to address reidentification. Possessing a key would actually make reidentification much easier, as the point of a key is to connect research subjects to the samples they contribute, and lacking the key would not prevent reidentification. Stewardships also do not address other privacy concerns such as improving informed consent and autonomy or reducing the potential for genetic discrimination. Although stewardships are more of an inconvenience to researchers rather than an actual impediment, they do so little, in practice, to protect privacy that they do not create a viable balance between the two.

## 2. Certificates of Confidentiality

Certificates of Confidentiality for research studies using genetic information are another means by which participants’ confidentiality could be (partially) protected. Certificates allow researchers to protect the privacy of their subjects by “withholding from all persons not connected with the . . . research the names or other identifying characteristics” of the study participants.<sup>177</sup> Specifically, researchers may not be compelled by law enforcement officials or in the context of any legal proceeding to identify subjects.<sup>178</sup> In a 1973 murder investigation, a Certificate successfully prevented disclosure of drug treatment program participants despite a grand jury subpoena for their photographs.<sup>179</sup>

However, the strength of Certificates was tested again in 2006 with less success.<sup>180</sup> A defense attorney was able to obtain access to

174. Taylor, *supra* note 70, at 33; Ingelfinger & Drazen, *supra* note 143.

175. Taylor, *supra* note 70, at 33.

176. Conley et al., *supra* note 137, at 347 (internal citations omitted).

177. 42 U.S.C. § 241(d) (2006).

178. *Id.*

179. *People v. Newman*, 298 N.E.2d 651, 657 (N.Y. 1973) (vacating adjudication of contempt against Dr. Robert Newman, then director of the New York City Methadone Maintenance Treatment Program, for refusing to comply with subpoena).

180. Laura M. Beskow et al., *Certificates of Confidentiality and the Compelled Disclosure of Research Data*, 322 SCIENCE 1054, 1054-55 (2008).

information about his client's participation in a research study, which had included collection of genetic information, conducted under a Certificate.<sup>181</sup> The court clearly was unfamiliar with Certificates and their intended imperviousness.<sup>182</sup>

Perhaps before courts can be expected to uphold the unimpeachable status of Certificates, additional legislation, and education, is necessary. However, the NIH still puts faith in their effectiveness and "explicitly encourages investigators" to obtain a Certificate as protection against compelled disclosure of participants in genome-wide association studies.<sup>183</sup>

In the context of research studies by DTC-GTCs, however, Certificates will usually be unavailable because they are limited to IRB-approved research.<sup>184</sup> In fact, most DTC-GTCs warn their clients that they may disclose personal information, including genetic information, if required to do so by law.<sup>185</sup> More importantly, the utility of Certificates for online-based genetic research studies will be limited because the greatest risks to individual privacy and confidentiality come from reidentification by technologically savvy computer users rather than from zealous attorneys. The request of a bioinformatician who demands that study participants be reidentified may be denied due to the presence of a Certificate, but one who does not bother to seek permission will not be thwarted. Additionally, Certificates do not address the privacy concerns of promoting informed consent and reducing genetic discrimination. Overall, Certificates are "insufficient to underwrite absolute privacy promises."<sup>186</sup>

#### *D. Interactive Informed Consent*

If we acknowledge the real threat of reidentification, but also that it is almost impossible to stop, we must concomitantly recognize that genetic research participants are vulnerable to breaches of privacy and anonymity. To ensure that the participants themselves are fully aware of this vulnerability, enhanced informed consent procedures should be implemented by Internet-based research studies. First, to approach full

---

181. *State v. Bradley*, 634 S.E.2d 258, 260 (N.C. 2006).

182. Beskow et al., *supra* note 180, at 1054.

183. NAT'L INSTS. OF HEALTH, POLICY FOR SHARING OF DATA OBTAINED IN NIH SUPPORTED OR CONDUCTED GENOME-WIDE ASSOCIATION STUDIES (GWAS) (2007), available at <http://grants.nih.gov/grants/guide/notice-files/NOT-OD-07-088.html>.

184. *But see supra* Part V.B.2 (suggesting an expansion of the Common Rule to cover DTC-GTCs, thus requiring IRB approval for research, and therefore opening up the availability of Certificates of Confidentiality).

185. *See, e.g., Terms of Service, supra* note 75, § 8.

186. Conley et al., *supra* note 137, at 349.

comprehension of risk, ignorance of risk must be acknowledged. Informed consent documents must fully disclose not only all known risks, including reidentification and genetic discrimination, but also state that there are unknown risks,<sup>187</sup> which may even be the most significant ones.<sup>188</sup> Second, these risks must be prominently displayed—perhaps in bolded text and all capital letters like waivers of liability are required to have—not buried in the fine print of an unread privacy policy.

The first ten enrollees in the PGP were required to have advanced degrees in genetics or similar fields to ensure that they fully appreciated the risks of their genetic information being made publicly available. The next wave of PGP subjects must submit to a lengthy and stringent screening process, including an entrance exam, to help ensure that they are similarly aware of the risks associated with public access to their genetic information. Other research consortiums and DTC-GTCs could also be required to include a screening process or entrance exam for their study participants.<sup>189</sup>

Another way to ensure that potential subjects fully appreciate the risks of participating is to prohibit companies from enrolling participants solely via the Internet. Interested individuals would be required to contact, preferably by phone rather than email, a genetic counselor on staff at the DTC-GTC<sup>190</sup> or research consortium who talks one-on-one with the subject, evaluates comprehension of possible risks, and answers questions.

Less radical, and more in sync with the online environment, is to leave consent procedures solely online, but implement something more robust than click-through forms. Currently, for example, a subject views a scroll-through screen full of caveats which he or she likely does not read before clicking the “I Consent” button at the bottom. Instead, subjects could be prompted to type a provided sentence that expresses comprehension of risk: “I, [enter your name], understand that by participating in this study, privacy and anonymity of my genetic information cannot be guaranteed and that someone, not authorized by me, may figure out that I participated in this study and may learn the content of my genetic information which could lead to discrimination or other negative effects.”

---

187. *Id.* at 354.

188. *See supra* text accompanying note 165.

189. *But see supra* Part IV.B (noting that consent procedures can decrease and therefore bias data sets).

190. Pathway Genomics currently appears to be the only DTC genetic testing company that provides its customers with access to genetic counselors pre- or post-testing, but the company does not have a research arm. PATHWAY GENOMICS, *supra* note 37.

The PGP is already using a similarly interactive tool, the multiple choice quiz, which interested participants must complete perfectly before being considered for enrollment. DTC-GTCs and research consortiums aside from the PGP could employ comparable online questionnaires that are designed to test comprehension of risk of study participation. Successful completion of these quizzes would help ensure that interested subjects read the consent forms and privacy statements well enough to appreciate the risks of their participation.

Overall, enhanced informed consent procedures strike a balance between protecting privacy and promoting research. Although consent procedures can inhibit research,<sup>191</sup> these enhanced requirements are not nearly as burdensome on researchers as the expansion of the Common Rule could be.<sup>192</sup> Additionally, although these procedures do not stop reidentification or genetic discrimination, they do acknowledge those potential adverse consequences. Armed with as much information as possible, research participants are less likely to suffer “post-enrollment regret.”<sup>193</sup>

## CONCLUSION

Both public and private Internet-based research studies provide the opportunity for individuals to contribute their genetic information to scientific and medical research projects, but the Internet also provides an environment in which individual privacy and anonymity are almost impossible to guarantee. Because so much can be gained from genetic research in the way of medical, scientific, and even bioinformatics advancements, participation should not be prohibited, but rather should be protected where possible and fully informed where protection is not possible. At a minimum, Congress should expand GINA to cover all genetic information, no matter how it is obtained. More importantly, online research studies should implement more robust enrollment procedures based on full disclosure of known potential risks (plus acknowledgment that others are unknown) and active, even interactive, acceptance of those risks by participants. Only then can we realize a true research revolution.

---

191. *See supra* Part IV.B.

192. *See supra* Part V.B.2.

193. Conley et al., *supra* note 137, at 354.

