AU BLR
American University Business Law Review
Volume 2 • 2013 • Issue 2

AMERICAN UNIVERSITY BUSINESS LAW REVIEW

The AMERICAN UNIVERSITY BUSINESS LAW REVIEW is published twice a year (fall and spring academic semesters) by students of the Washington College of Law, American University, 4801 Massachusetts Avenue, N.W., Suite 615A, Washington, D.C. 20016. Manuscripts should be sent to the Executive Editor at the above listed address or electronically at blr-ee@wcl.american.edu.

Subscription rate per year: $45.00 domestic, $50.00 foreign, $30.00 alumni, $20.00 single issue. Periodicals postage paid at Washington, D.C., and additional mailing offices. Office of Publication: 4801 Massachusetts Avenue, N.W., Suite 615A, Washington, D.C. 20016. Printing Office: Joe Christensen, Inc., 1540 Adams Street, Lincoln, Nebraska 68521. POSTMASTER: Send address changes to the AMERICAN UNIVERSITY BUSINESS LAW REVIEW, 4801 Massachusetts Avenue, N.W., Suite 615A, Washington, D.C. 20016.

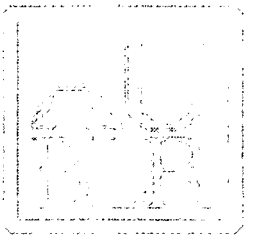
Subscriptions are renewed automatically on expiration unless cancellation is requested. It is our policy that unless a claim is made for nonreceipt of the AMERICAN UNIVERSITY BUSINESS LAW REVIEW issues within six months of the mailing date, the *American University Business Law Review* cannot be held responsible for supplying those issues without charge.

Citations conform generally to *The Bluebook: A Uniform System of Citation* (19th ed. 2010).
To be cited as: 2 AM. U. BUS. L. REV.

American University Business Law Review
Print ISSN 2168-6890
Online ISSN 2168-6904

AMERICAN UNIVERSITY BUSINESS LAW REVIEW

VOLUME 2 · 2013 · ISSUE 2



AMERICAN UNIVERSITY
WASHINGTON COLLEGE OF LAW FACULTY

Administration

Claudio M. Grossman, B.A., J.D., Doctor of Science of Law, *Dean*
Anthony E. Varona, A.B., J.D., LL.M., *Associate Dean of Faculty and Academic Affairs*
Mary L. Clark, A.B., J.D., LL.M., *Associate Dean of Faculty and Academic Affairs*
David B. Jaffe, B.A., J.D., *Associate Dean of Student Affairs*
Ruth Swanson, B.M., *Associate Dean of Development and Alumni Relations*
*Billie Jo Kaufman, B.S., M.S., J.D., *Associate Dean of Library and Information Resources*
Robert D. Dinerstein, A.B., J.D., *Associate Dean of Experiential Education and Director of Clinical Programs*
Stephen I. Vladeck, B.A., J.D., *Associate Dean of Scholarship*
Khalid R. O. Khalid, B.A., M.A., *Assistant Dean of Finance and Administration*
Rebecca T. Davis, B.S., M.A.T, *Assistant Dean of Academic Services and Registrar*
D. Akira Shiroma, B.A., J.D., *Assistant Dean of Admissions and Financial Aid*
Traci Mundy Jenkins, B.A., J.D., *Assistant Dean for Career and Professional Development*
Lia Epperson, B.A., J.D., *Director of the S.J.D. Program*
David Hunter, B.A., J.D., *Director of the International Legal Studies Program*
Jamin B. Raskin, B.A., J.D., *Director of the Law and Government Program*
David E. Aaronson, B.A., M.A., Ph.D., *Director of the Trial Advocacy Program*
Teresa Godwin Phelps, B.A., M.A., M.S.L, Ph.D., *Director of the Legal Rhetoric Program*
Ann Shalleck, A.B., J.D., *Director of the Women and the Law Program*

Full-Time Faculty

David E. Aaronson, B.A., M.A., Ph.D., The George Washington University; LL.B., Harvard University; LL.M., Georgetown University. *B. J. Tennery Professor of Law and Director of the Trial Advocacy Program*
Evelyn G. Abravanel, A.B., J.D., Case Western Reserve University. *Professor of Law*
Padideh Ala'i, B.A., University of Oregon; J.D., Harvard University. *Professor of Law*
Jonas Anderson, B.S., University of Utah; J.D., Harvard University. *Assistant Professor of Law*
*Kenneth Anderson, B.A., University of California–Los Angeles; J.D., Harvard University. *Professor of Law* (on leave Spring 2013)
Isaiah Baker, B.A., Yale University; M.A., DePaul University; M.B.A., J.D., Columbia University; LL.M., Harvard University. *Associate Professor of Law* (on leave 2012-2013)
Jonathan B. Baker, A.B., J.D., Harvard University; M.A., Ph.D., Stanford University. *Professor of Law*
Susan D. Bennett, B.A., M.A., Yale University; J.D., Columbia University. *Professor of Law*
Daniel Bradlow, B.A., University of Witwatersrand, South Africa; J.D., Northeastern University; LL.M., Georgetown University. *Professor of Law* (on leave Spring 2013)
Pamela Bridgewater, B.S., Florida Agricultural and Mechanical University; J.D., Florida State University; LL.M., University of Wisconsin. *Professor of Law* (on leave 2012-2013)
Barlow Burke Jr., A.B., Harvard University; LL.B., MCP, University of Pennsylvania; LL.M., S.J.D., Yale University. *Professor of Law and John S. Myers and Alvina Reckman Myers Scholar*
Susan D. Carle, A.B., Bryn Mawr College; J.D., Yale University. *Professor of Law*
Michael W. Carroll, A.B., University of Chicago; J.D., Georgetown University. *Professor of Law and Director of the Program on Information Justice and Intellectual Property*
David F. Chavkin, B.S., Michigan State University; J.D., University of California, Berkeley. *Professor of Law* (on leave Spring 2013)
Janie Chuang, B.A., Yale University; J.D., Harvard University. *Associate Professor of Law*
Mary Clark, A.B., Bryn Mawr College; J.D., Harvard University, LL.M., Georgetown University. *Professor of Law and Associate Dean of Faculty and Academic Affairs*
Jorge Contreras, B.S.EE, B.A., Rice University; J.D., Harvard University. *Associate Professor of Law*
John B. Corr, B.A., M.A., John Carroll University; Ph.D., Kent State University; J.D., Georgetown University. *Professor of Law*
Angela Jordan Davis, B.A., Howard University; J.D., Harvard University. *Professor of Law*
Amy Dillard, B.A., Wellesley College; J.D., Washington and Lee University. *Visiting Assistant Professor of Law* (Spring 2013)
Robert D. Dinerstein, A.B., Cornell University; J.D., Yale University. *Professor of Law, Associate Dean of Experiential Education, and Director of Clinical Programs*
N. Jeremi Duru, B.A., Brown University; M.P.P., J.D., Harvard University, *Professor of Law* (Spring 2013)
*Walter A. Effross, A.B., Princeton University; J.D., Harvard University. *Professor of Law and Director of the Program on Counseling Electronic Commerce Entrepreneurs*

Lia Epperson, B.A., Harvard University; J.D., Stanford University.
Associate Professor of Law and Director of the S.J.D. Program

*Christine Haight Farley, B.A., State University of New York, Binghamton;
J.D., State University of New York, Buffalo; LL.M., J.S.D., Columbia University.
Professor of Law (on leave Spring 2013)

Amanda Frost, B.A., J.D., Harvard University. *Professor of Law*

*Anna Gelpern, A.B., Princeton University; J.D., Harvard University. *Professor of Law* (on leave Fall 2012)

Robert K. Goldman, B.A., University of Pennsylvania; J.D., University of Virginia.
Professor of Law and Louis C. James Scholar

Claudio M. Grossman, Licenciado en Ciencias Juridicas y Sociales, Universidad de Chile, Santiago;
Doctor of Science of Law, University of Amsterdam. *Dean, Professor of Law, and Raymond I. Geraldson Scholar for International and Humanitarian Law*

Lewis A. Grossman, B.A., Ph.D., Yale University; J.D., Harvard University. *Professor of Law*

*Heather L. Hughes, B.A., University of Chicago; J.D., Harvard University. *Professor of Law*

David Hunter, B.A., University of Michigan; J.D., Harvard University.
Professor of Law and Director of the International Legal Studies Program

Darren L. Hutchinson, B.A., University of Pennsylvania; J.D., Yale University.
Professor of Law (on leave 2012-2013)

Peter A. Jaszi, A.B., J.D., Harvard University.
Professor of Law and Faculty Director of the Glushko-Samuelson Intellectual Property Clinic

Cynthia E. Jones, B.A., University of Delaware; J.D., American University. *Associate Professor of Law*

*Billie Jo Kaufman, B.S., M.S., University of Indiana–Bloomington; J.D., Nova Southeastern University.
Professor of Law and Associate Dean of Library and Information Resources

Nicholas N. Kittrie, M.A., LL.B., University of Kansas; LL.M., S.J.D., Georgetown University.
University Professor (on leave Fall 2012)

Nancy J. Knauer, B.A., J.D., University of Pennsylvania. *Visiting Professor of Law* (Spring 2013)

Benjamin Leff, B.A., Oberlin College; A.M., University of Chicago; J.D., Harvard University.
Associate Professor of Law

Amanda Cohen Leiter, B.S., M.S., Stanford University; M.S., University of Washington; J.D., Harvard University.
Associate Professor of Law

James P. May, B.A., Carleton College; J.D., Harvard University. *Professor of Law*

Juan E. Mendez, LL.B., Stella Maris Catholic University, Argentina. *Visiting Professor of Law* (2012-2013)

Binny Miller, B.A., Carleton College; J.D., University of Chicago. *Professor of Law*

Elliott S. Milstein, B.A., University of Hartford; J.D., University of Connecticut; LL.M., Yale University.
Professor of Law

Carl C. Monk, B.A., Oklahoma State University; J.D., Howard University. *Visiting Professor of Law* (2012-2013)

Fernanda Nicola, B.A., University of Turin; Ph.D., Trento University; LL.M., Harvard University.
Associate Professor of Law

Diane F. Orentlicher, B.A., Yale University; J.D., Columbia University. *Professor of Law*

Teresa Godwin Phelps, B.A., M.A., Ph.D., University of Notre Dame; M.S.L, Yale University.
Professor of Law and Director of the Legal Rhetoric Program (on leave Fall 2012)

*Andrew D. Pike, B.A., Swarthmore College; J.D., University of Pennsylvania. *Professor of Law*

Nancy D. Polikoff, B.A., University of Pennsylvania; M.A., The George Washington University;
J.D., Georgetown University. *Professor of Law* (on leave Fall 2012)

Andrew F. Popper, B.A., Baldwin Wallace College; J.D., DePaul University;
LL.M., The George Washington University. *Professor of Law*

Jamin B. Raskin, B.A., J.D., Harvard University.
Professor of Law and Director of the Law and Government Program

Jayesh Rathod, A.B., Harvard University; J.D., Columbia University.
Associate Professor of Law and Director of the Immigrant Justice Clinic

Ira P. Robbins, A.B., University of Pennsylvania; J.D., Harvard University.
Professor of Law and Justice, Director of the J.D./M.S. Dual Degree Program in Law and Justice, and Barnard T. Welsh Scholar

Jenny Roberts, B.A., Yale University; J.D., New York University. *Professor of Law*

Ezra Rosser, B.A., Yale University; J.D., Harvard University. *Professor of Law* (on leave Fall 2012)

Herman Schwartz, A.B., J.D., Harvard University. *Professor of Law*

Ann Shalleck, A.B., Bryn Mawr College; J.D., Harvard University.
Professor of Law, Director of the Women and the Law Program, and Carrington Shields Scholar

*Mary Siegel, A.B., Vassar College; J.D., Yale University. *Professor of Law*

Rita J. Simon, B.A., University of Wisconsin; Ph.D., University of Chicago. *University Professor*

Brenda V. Smith, B.A., Spelman College; J.D., Georgetown University. *Professor of Law*

*David Snyder, B.A., Yale University; J.D., Tulane University.
Professor of Law and Director of the Law and Business Program
Andrew E. Taslitz, B.A., City University of New York; J.D., University of Pennsylvania. *Professor of Law*
Robert L. Tsai, B.A., University of California–Los Angeles; J.D., Yale University. *Professor of Law*
Anthony E. Varona, A.B., J.D., Boston College; LL.M., Georgetown University.
Professor of Law and Associate Dean of Faculty and Academic Affairs
Robert G. Vaughn, B.A., J.D., University of Oklahoma; LL.M., Harvard University.
Professor of Law and A. Allen King Scholar
Stephen I. Vladeck, B.A., Amherst College; J.D., Yale University.
Professor of Law and Associate Dean of Scholarship
Perry Wallace Jr., B.S., Vanderbilt University; J.D., Columbia University.
Professor of Law and Director of the J.D./M.B.A. Dual Degree Program (on leave Fall 2012)
Lindsay F. Wiley, A.B., J.D., Harvard University; M.P.H., Johns Hopkins University.
Assistant Professor of Law
Paul R. Williams, A.B., University of California–Davis; J.D., Stanford University.
Professor of International Service and Director of the J.D./M.B.A. Dual Degree Program
Richard J. Wilson, B.A., DePauw University; J.D., University of Illinois.
Professor of Law and Director of the International Human Rights Law Clinic

Law Library Administration

Christine K. Dulaney, B.A., State University of New York at Buffalo; M.A., University of Virginia; M.L.S., University of Chicago. *Associate Law Librarian*
John Q. Heywood, B.S., Northern Arizona University; J.D., American University. *Associate Law Librarian*
*Billie Jo Kaufman, B.S., M.S., University of Indiana–Bloomington; J.D., Nova Southeastern University. *Associate Dean of Library and Information Resources*
Susan Lewis, B.A., University of California–Los Angeles; J.D., Southwestern University; M.Lbr., University of Washington. *Law Librarian*
Sima Mirkin, B.S.c, Byelorussian Polytechnic Institute, Minsk, Belarus; M.L.S., University of Maryland.
Associate Law Librarian
Adeen Postar, A.B., J.D., Washington University; M.S.L.S., The Catholic University of America. *Law Librarian*
William T. Ryan, B.A., Boston University; J.D., American University; M.L.S., University of Maryland. *Law Librarian*
John A. Smith, B.A., St. Michaels College; M.S.L.S., The Catholic University of America. *Assistant Law Librarian*
Amy Taylor, B.A., Rhodes College; M.S.L.I.S., The Catholic University of America; J.D., The University of Alabama. *Associate Law Librarian*
Ripple L. Weistling, B.A., Brandeis University; M.A., King's College, London, England; J.D., Georgetown University; M.S.L.S., The Catholic University of America. *Assistant Law Librarian*

Emeriti

Egon Guttman, LL.B., LL.M., University of London. *Professor of Law and Levitt Memorial Trust Scholar Emeritus*
Candace S. Kovacic-Fleischer, A.B., Wellesley College; J.D., Northeastern University. *Professor Law Emeritus*
Patrick E. Kehoe, B.C.S., Seattle University; J.D., MLLibr, University of Washington. *Law Librarian Emeritus*
Robert B. Lubic, A.B., J.D., University Pittsburgh; MPL, Georgetown University. *Professor of Law Emeritus*
Gary McCann, B.A., California State University; J.D., Willamette University; M.L.S., University of Texas.
Law Librarian Emeritus
Margaret Mitchell Milam, B.A., M.L.S., University of Maryland; J.D., American University. *Law Librarian Emerita*
Anthony C. Morella, A.B., Boston University; J.D., American University. *Professor of Law Emeritus*
Michael E. Tigar, B.A., J.D., University of California, Berkeley. *Professor of Law Emeritus*
Joanne A. Zich, B.A., Washington University; M.LS, Columbia University. *Librarian Emerita*

Special Faculty Appointments

Nancy S. Abramowitz, B.S., Cornell University; J.D., Georgetown University. *Professor of Practice of Law*
David Baluarte, B.A., Brown University; J.D., American University. *Practitioner in Residence*
Elizabeth Beske, B.A., Princeton University; J.D., Columbia University. *Legal Writing Instructor in Residence*
Elizabeth Boals, B.S., Virginia Polytechnic Institute and State University; J.D., George Mason University.
Associate Director of the Trial Advocacy Program
Llezlie Green Coleman, A.B., Dartmouth College; J.D., Columbia University. *Practitioner in Residence*
Gary J. Edles, B.A., City University of New York; J.D., New York University; LL.M., S.J.D., The George Washington University. *Fellow in Administrative Law*
Paul Figley, B.A., Franklin and Marshall College; J.D., Southern Methodist University.
Legal Writing Instructor in Residence
Sean Flynn, B.A., Pitzer College; J.D., Harvard University. *Professorial Lecturer in Residence*

Jon Gould, A.B., University of Michigan; M.P.P., J.D., Harvard University; Ph.D., University of Chicago.
Professor, Department of Justice, Law and Society and Affiliate Professor of Law
Jasmine Harris, B.A., Dartmouth College; J.D., Yale University. *Practitioner in Residence*
Nabila Isa-Odidi, B.S., University of Toronto; J.D., American University. *Practitioner in Residence*
Elizabeth A. Keith, B.A., University of North Carolina, Chapel Hill; J.D., George Mason University.
Legal Writing Instructor in Residence
Daniela Kraiem, B.A., University of California–Santa Barbara; J.D., University of California–Davis.
Associate Director of the Women and the Law Program
Jerome I. Levinson, B.A., LL.B., Harvard University. *Distinguished Lawyer in Residence*
Jeffrey S. Lubbers, A.B., Cornell University; J.D., University of Chicago. *Professor of Practice of Administrative Law*
Daniel Marcus, B.A., Brandeis University; LL.B., Yale University. *Fellow in Law and Government*
Claudia Martin, J.D., Universidad de Buenos Aires; LL.M., American University. *Professorial Lecturer in Residence*
Jennifer Mueller, B.A., University of North Carolina, Chapel Hill; J.D., Harvard University. *Practitioner in Residence*
Nantasa Nanasi, B.A. Brandeis University; J.D., Georgetown University. *Practitioner in Residence*
Horacio A. Grigera Naon, J.D., LLD, University of Buenos Aires; LL.M., S.J.D., Harvard University.
Distinguished Practitioner in Residence
Victoria Phillips, B.A., Smith College; J.D., American University. *Professor of Practice of Law*
Heather E. Ridenour, BB.A., Texas Women's University; J.D., Texas Wesleyan University.
Director of Academic Support and Legal Writing Instructor in Residence
Diego Rodriguez-Pinzon, J.D., Universidad de los Andes; LL.M., American University;
S.J.D., The George Washington University. *Professorial Lecturer in Residence*
Susana SaCouto, B.A., Brown University; J.D., Northeastern University; M.A.LD, Tufts University.
Professorial Lecturer in Residence
Macarena Saez, Licenciada en Ciencias Juridicas y Sociales, University of Chile; LL.M., Yale University.
Fellow in International Legal Studies
Anita Sinha, B.A.,Barnard College; J.D., New York University. *Practitioner in Residence*
William Snape, B.A., University of California–Los Angeles; J.D., The George Washington University.
Director of Adjunct Faculty Development and Fellow in Environmental Law
David H. Spratt, B.A., The College of William and Mary; J.D., American University.
Legal Writing Instructor in Residence
Shana Tabak, B.A., Macalaster College; J.D., Georgetown University; LL.M., The George Washington University.
Practitioner in Residence
Richard S. Ugelow, B.A., Hobart College; J.D., American University; LL.M., Georgetown University.
Practitioner in Residence
L. Rangeley Wallace, B.A., Emory University; J.D., American University;
LL.M., Georgetown University (Spring 2013).
Stephen Wermiel, B.A., Tufts University; J.D., American University. *Fellow in Law and Government*
Sofia Yakren, B.A., J.D., Yale University. *Practitioner in Residence*
William R. Yeomans, B.A., Trinity College, Connecticut; J.D., Boston University; LL.M., Harvard University.
Fellow in Law and Government

* *American University Business Law Review* Faculty Advisory Committee

ARTICLES

FIDDLING ON THE ROOF: RECENT DEVELOPMENTS IN CYBERSECURITY

MELANIE J. TEPLINSKY*

TABLE OF CONTENTS

* Ms. Teplinsky is an adjunct professorial lecturer at American University Washington College of Law ("WCL"). She also serves on the Advisory Board of CrowdStrike, Inc. and writes and speaks frequently on cyberlaw issues. Prior to joining WCL, Ms. Teplinsky practiced law at Steptoe & Johnson LLP, where she counseled leading financial services, telecommunications, and other multinational clients on a wide array of issues including cybersecurity, data protection, and electronic surveillance. Ms. Teplinsky is a graduate of Harvard Law School and served as a law clerk to the Honorable Judge Rya W. Zobel, U.S. District Court, District of Massachusetts. The author wishes to thank Arjun Prasad and the editorial staff of the *American University Business Law Review* for their exceptional work and gratefully acknowledges Dmitri Alperovitch and Steven Chabinsky, who have contributed significantly to the author's thinking about the future of U.S. cybersecurity policy. The author also wishes to thank her family for their forbearance as she worked on this article, especially her loving and supportive husband, Steven, and their six-year-old red-headed daughter, who missed mommy so much during the drafting of this Article that she asked mommy to "pinky promise" not to write another.

INTRODUCTION

[Y]ou might say every one of us is a fiddler on the roof trying to scratch out a pleasant, simple tune without breaking his neck.
-Fiddler on the Roof[1]

For today's CEOs and corporate boards of directors, trying to capture the benefits of new technology while tackling emerging cybersecurity challenges is a delicate balance akin to fiddling on the roof. This Article outlines recent developments in ".com" cybersecurity and their implications for corporate cybersecurity. Section I summarizes how information technologies have revolutionized the functioning of global economies, societies, and governments. Section II discusses the U.S. self-regulatory approach to ".com" cybersecurity and the long-standing challenge of securing critical infrastructure ("CI") networks. Sections III–V discuss technology trends, the cyberthreat landscape, and legislative developments affecting cybersecurity, respectively. Specifically, Section III outlines three technological trends that pose cybersecurity challenges: explosive growth in mobile technology; migration to cloud computing; and increasing pervasiveness of social networks. Section IV examines the increasingly complex global cyberthreat landscape, including the problems of cybercrime, cyberespionage, and cyberwarfare. Section V discusses recent congressional and executive action on cybersecurity, including the ongoing congressional debate over cybersecurity legislation. Finally, Sections VI and VII describe private sector cybersecurity challenges and opportunities, including the potential for the private sector to shift the long-standing ".com" cybersecurity debate in Washington toward a more holistic strategy that encompasses not only vulnerability mitigation, but also deterrence.

I. THE PROMISE AND PERIL OF CYBERSPACE

It has been said that "[c]yberspace touches practically everything and everyone."[2] With over two billion people relying on the Internet[3] for a

1. FIDDLER ON THE ROOF (United Artists 1971).

2. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE i (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [hereinafter WHITE HOUSE, CYBERSPACE POLICY REVIEW].

3. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011), http://www.defense.gov/news/d20110714cyber.pdf. ("From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people.").

wide variety of economic,[4] social,[5] and political interactions,[6] cyberspace—the "globally-interconnected digital information and communications infrastructure"[7]—is nothing short of essential to modern life.

Information technologies ("IT") have revolutionized the functioning of economies, societies, and governments around the globe. First, by any measure, IT has transformed the way we conduct business. IT has fundamentally changed the relationship between businesses and consumers, allowing not only for improved market differentiation and personalization of services, but also for the transformation of marketing through social media.[8] Internally, IT has driven business efficiency through the automation and/or reorganization of business processes, such as invoicing, recordkeeping, and supply chain management;[9] big data analytics;[10] and the

4. Global e-commerce sales are expected to reach $963 billion by 2013, according to Goldman Sachs projections. Don Davis, *Global e-Commerce Sales Head for the $1 Trillion Mark*, INTERNET RETAILER (Jan. 4, 2011, 3:02 PM), http://www.internetretailer.com/2011/01/04/global-e-commerce-sales-head-1-trillion-mark. *Cf.* SUCHARITA MULPURU ET AL., FORRESTER, THE ECOMMERCE JUGGERNAUT DOMINATES RETAIL 1 (2012) (noting that global e-commerce will represent a "trillion-dollar opportunity" by 2016). By 2016, Forrester predicts that "more than half of the dollars spent in U.S. retail will be influenced by the Web." SUCHARITA MULPURU ET AL., FORRESTER, US CROSS-CHANNEL RETAIL FORECAST, 2011 TO 2016 (2012).

5. *See, e.g.*, *The Local Network: Experian Analysis Highlights Which Countries Spend Longest on Facebook*, EXPERIAN (Sept. 27, 2011), http://www.experianplc.com /news/company-news/2011/27-09-2011.aspx ("Social networking is now one of the biggest online pastimes across the globe.").

6. Claire Cain Miller, *How Obama's Campaign Changed Politics*, N. Y. TIMES BITS BLOG (Nov. 7, 2008, 7:49 PM), http://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics ("Mr. Obama used the Internet to organize his supporters in a way that would have in the past required an army of volunteers and paid organizers on the grounds . . . . Were it not for the Internet, Barack Obama would not be president."); *see* Megan Garber, *The Campaign Tumblr Is Dead! (Long Live the Campaign Tumblr!)*, THE ATLANTIC (Nov. 28, 2012, 5:33 PM), http://www.theatlantic.com/technology/archive/2012/11/the-campaign-tumblr-is-dead-long-live-the-campaign-tumblr/265688/ (discussing the first presidential campaign Tumblr).

7. WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at iii.

8. Jessica Bosari, *The Developing Role of Social Media in the Modern Business World*, FORBES (Aug. 8, 2012, 12:26 PM), http://www.forbes.com/sites /moneywisewomen/2012/08/08/the-developing-role-of-social-media-in-the-modern-business-world/ (asserting that social media marketing has become a "must" and citing a recent survey finding that "94% of all businesses with a marketing department used social media as part of their marketing platform").

9. Victoria Taylor, *Supply Chain Management: The Next Big Thing*, BLOOMBERG BUSINESSWEEK (Sept. 12, 2011), http://www.businessweek.com/business-schools/supply-chain-management-the-next-big-thing-09122011.html.

10. David Feinleib, *The 3 I's of Big Data*, FORBES (July 9, 2012, 4:05 PM), http://www.forbes.com/sites/davefeinleib/2012/07/09/the-3-is-of-big-data/ ("Big Data is . . . a transformative set of technological advances that have made analyzing data vastly more efficient."); Charles Duhigg, *How Companies Learn Your Secrets*, N.Y.

adoption of electronic payment solutions.[11] Moreover, the deployment of telecommunications technologies (e.g., videoconferencing) and collaborative software has reduced unnecessary business travel and improved collaboration across borders and time zones.

Second, IT has transformed societies. We work, shop,[12] and socialize[13] online. We embrace information technology's promise of improved healthcare (e.g., through personalized medicine,[14] telemedicine,[15] health-related mobile applications,[16] and big data analytics[17]), greater

---

TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all (describing major retailers' use of big data analytics to more efficiently market to consumers).

11. *See* Greg McAllister, *Mobile Payments: The Case for Choosing an Open Platform*, FORBES (Nov. 24, 2012, 8:44 PM), http://www.forbes.com/sites/ciocentral/2012/11/24/mobile-payments-the-case-for-choosing-an-open-platform/ (referencing efficiencies through mobile payments); MASTERCARD WORLDWIDE, BENEFITS OF OPEN PAYMENT SYSTEMS AND THE ROLE OF INTERCHANGE 8 (2008), http://www.mastercard.com/us/company/en/docs/BENEFITS%20OF%20ELECTRONIC%20PAYMENTS%20-%20US%20EDITION.pdf ("[Merchants using electronic payments] benefit by reducing costs associated with handling other forms of payment, including bounced checks, check verification and guarantee services, and check processing [as well as] collecting, counting, and transporting [cash].").

12. *See* Alistairr Barr, *Cyber Monday sales best ever, for Amazon's Kindle too*, CHI. TRIB. (Nov. 27, 2012), http://www.chicagotribune.com/business/sns-rt-us-amazon-kindlebre8aq0qt-20121127,0,4261081.story ("Internet sales jumped 30.3% on Cyber Monday [November 26, 2012] making it the biggest online shopping day ever. . . .").

13. JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF ONLINE SOCIALIZING 1 (2010), http://pewresearch.org/pubs/1652/social-relations-online-experts-predict-future ("[E]mail, social networks, and other online tools offer 'low friction' opportunities to create, enhance, and rediscover social ties that make a difference in people's lives. The internet lowers traditional communications constraints of cost, geography, and time; and it supports the type of open information sharing that brings people together.").

14. *See generally* DARRELL M. WEST, CTR. FOR TECH. INNOVATION AT BROOKINGS, ENABLING PERSONALIZED MEDICINE THROUGH HEALTH INFORMATION TECHNOLOGY: ADVANCING THE INTEGRATION OF INFORMATION 1 (2011), http://www.brookings.edu/~/media/research/files/papers/2011/1/28%20personalized%20medicine%20west/0128_personalized_medicine_west.pdf (discussing the challenges and concerns of implementing personalized healthcare through technology and offering possible solutions).

15. *See* Pam Belluck, *With Telemedicine as Bridge, No Hospital Is an Island*, N.Y. TIMES (Oct. 8, 2012), http://www.nytimes.com/2012/10/09/health/nantucket-hospital-uses-telemedicine-as-bridge-to-mainland.html?pagewanted=all&r=0.

16. *See* Joshua Brustein, *Coming Next: Using an App as Prescribed*, N.Y. TIMES (Aug. 19, 2012), http://www.nytimes.com/2012/08/20/technology/coming-next-doctors-prescribing-apps-to-patients.html.

17. Derrick Harris, *Better Medicine, Brought to You By Big Data*, GIGAOM (July 15, 2012, 6:00 AM), http://gigaom.com/cloud/better-medicine-brought-to-you-by-big-data/ (discussing the potential impact of big data analytics on genomics and current health-related applications for big data analytics including an effort to treat pediatric

democratization,[18] and improved quality of life for ourselves as individuals and as societies.[19]

Third, at the nation-state level, governments increasingly rely on IT solutions to provide cheaper, more efficient delivery of government services through e-government initiatives;[20] to manage their own supply chains;[21] to facilitate online voting;[22] and to carry out essential government functions, such as national defense.[23]

---

cancer based on the individual genetic profile of each affected child).

18. *See* RICHARD HUNDLEY ET AL., THE GLOBAL COURSE OF THE INFORMATION REVOLUTION: RECURRING THEMES AND REGIONAL VARIATIONS, RAND CORP. xxvii (2003), http://www.rand.org/content/dam/rand/pubs/monographreports/MR1680/MR1680.sum.pdf ("New political actors are being empowered by the information revolution—in the business, social, and political realms, at the subnational, transnational, and supranational levels—which is changing the distribution of political power.").

19. Press Release, United Nations, Information technology must be used to improve life in poor countries - Annan (Sept. 12, 2003), *available at* http://www.un.org/apps/news/story.asp?NewsID=8227&Cr=information&Cr1=technology (describing a video message from then-U.N. Secretary General Kofi Annan imploring UN Information and Communications Technology Task Force members to "spread the word" at the 2003 World Summit on the Information Society "about initiatives that make creative use of technology to improve the quality of life in developing countries").

20. *See* OFFICE OF E-GOV'T & INFO. TECH., OFFICE OF MGMT. & BUDGET, DIGITAL GOVERNMENT: BUILDING A 21ST CENTURY PLATFORM TO BETTER SERVE THE AMERICAN PEOPLE 27 (2012), http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf (describing the Obama Administration's strategy for "harnessing the power of technology to help create a 21st century digital government—one that is efficient, effective and focused on improving the delivery of services to the American people").

21. *See* HUNDLEY ET AL., *supra* note 18, at xxvii.

22. Although not generally accepted in the United States, other countries, such as the United Kingdom, Estonia, Switzerland, and Canada, have all begun to use Internet voting. Joanna Stern, *Why You Cannot Vote Online Today*, ABC NEWS (Nov. 6, 2012), http://abcnews.go.com/Politics/OTUS/election-day-vote-online-internet-today/story?id=17647954#.ULTveo4QgqY.

23. CHARLES BILLO & WELTON CHANG, INST. FOR SEC. TECH. STUDIES AT DARMOUTH COLL., CYBER WARFARE: AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES 3 (2004), http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf ("Information processing is becoming a 'center of gravity' in future warfare."); U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT 1 (2011), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf ("Cyberspace is a critical enabler to Department of Defense (DoD) military, intelligence, business and, potentially, civil support operations."); BRYAN KREKEL ET AL., NORTHROP GRUMMAN CORP., OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE 10 (2012), http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf (describing the United States military's reliance on IT for vital "C4ISR" (i.e., command, control, communications, computers, intelligence, surveillance, and reconnaissance functions)); *see* COL. JASON SPADE, U.S.

Finally, at the international level, the growing global reliance on cyberspace has implications for established governance models,[24] alliances,[25] international stability,[26] and warfare.[27]

As we work to realize the extraordinary promise of cyberspace, we face

---

ARMY WAR COLL., INFORMATION AS POWER: CHINA'S CYBER POWER AND AMERICA'S NATIONAL SECURITY 25 (Jeffrey Caton ed., 2012), http://www.carlisle.army.mil/dime/documents/China's%20Cyber%20Power%20and%20America's%20National%20Security%20Web%20Version.pdf ("The U.S. military is particularly cyber dependent, relying on a global network of 15,000 local area networks and 7 million computers connected by over 100,000 telecommunication circuits, spread across bases worldwide.").

24. *See* HUNDLEY ET AL., *supra* note 18, at xxvi ("Some traditional mechanisms of governance (e.g., taxation, regulation and licensing) are becoming increasingly problematic as the information revolution allows action beyond the reach of national governments."); Violet Blue, *U.S. Now 'Totally Unified' in Opposition to U.N. Internet Governance*, ZDNET (Dec. 6. 2012, 12:52 AM), http://www.zdnet.com/u-s-now-totally-unified-in-opposition-of-u-n-internet-governance-7000008382/ (reporting that, as the U.N.'s International Telecommunications Union considered proposals from various countries dealing with Internet regulation during the WCIT-12 summit in Dubai, the House of Representatives unanimously passed (397-0) a resolution intended to send a signal that the White House and Congress opposed any role the U.N. might take in Internet governance or regulation).

25. *See* NATO, DEFENDING THE NETWORKS: NATO POLICY ON CYBER DEFENCE (2011), http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf (providing a coordinated approach to cyberdefense across the NATO Alliance); Press Release, NATO, Lisbon Summit Declaration (Nov. 20, 2010), *available at* http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease ("Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance . . . ."); NATO, STRATEGIC CONCEPT FOR THE DEFENCE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANISATION, ACTIVE ENGAGEMENT, MODERN DEFENCE ¶ 19 (2010), http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf ("We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will: . . . develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations . . . .").

26. FRANKLIN D. KRAMER, ATLANTIC COUNCIL, ACHIEVING INTERNATIONAL CYBER STABILITY 14 (2012), http://www.acus.org/files/publication_pdfs/403/kramer_cyber_final.pdf (noting the establishment of a "cyber hot line" between the United States and Russia, and arguing that better resilience, cooperation, and transparency are necessary to enhance international cyber stability).

27. *See generally The Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO COOPERATIVE CYBER DEF. CENTRE OF EXCELLENCE, https://www.ccdcoe.org/249.html (last visited Mar. 27, 2013) (announcing the publication of the "Tallinn Manual," the result of a "three-year effort to examine how extant international law norms" apply to cyberwarfare).

an extraordinary challenge. Our shared digital infrastructure is vulnerable[28] to a wide-range of cyberthreats that are understood to pose some of the most serious economic and national security challenges of the 21st century (see *infra* Section IV).

II. SELF-REGULATION AND THE CHALLENGE OF CRITICAL INFRASTRUCTURE

The United States has adopted a largely self-regulatory, market-based approach to cybersecurity, relying on the private sector to secure its own networks. In keeping with this approach, no federal agency is responsible for defending the civilian (i.e., ".com") domain, and the federal government has avoided generally-applicable federal mandates regarding private sector cybersecurity practices.[29] Private sector companies have long understood that perfect security is unattainable, and, even if that were not the case, would be cost-prohibitive.[30] Accordingly, they must decide for themselves the optimal level of cybersecurity investment on a company-by-company basis.

A key challenge to the prevailing self-regulatory approach to private sector cybersecurity is the special problem of "critical infrastructures."[31] As explained in the National Strategy to Secure Cyberspace, which the

28. WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at iii; *see* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 4 (2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE] (describing digital infrastructure vulnerability to "natural disasters, accidents, and sabotage").

29. Companies handling certain types of sensitive personal data may be subject to sector-specific information security rules and also should be aware that the FTC has, under certain circumstances, set and enforced corporate data security obligations through both litigation and consent orders under its statutory authority to regulate "unfair" and "deceptive" trade practices pursuant to Section 5 of the FTCA. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, No. 12-cv-01365-SPL (D. Ariz. filed June 26, 2012), discussed in greater detail *infra* Section V.E.

30. *See, e.g.*, U.S. CHAMBER OF COMMERCE, INTERNET SECURITY ESSENTIALS FOR BUSINESS 2.0, at 3 (2012), http://www.uschamber.com/issues/technology/internet-security-essentials-business ("Perfect online security is unattainable . . . ."); *Public Fears in Virtual Places: Inaugural Cyber Security Lecture Tackles Crime, Solutions*, CABLE (July 21, 2012, 3:14 PM), http://cable.poly.edu/issue/news/public-fears-virtual-places-inaugural-cyber-security-lecture-tackles-crime-solutions (according to Marcus Sachs, Vice President of government affairs and national security policy at Verizon Communications, "perfection is impossible" and failures in cybersecurity are "inevitable").

31. Critical infrastructures are the "systems and assets, whether physical or virtual, so vital to the United States that the [incapacitation] or destruction of such systems and assets would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (Supp. V 2011).

Department of Homeland Security ("DHS") released in 2003 in response to the 9/11 terrorist attacks:

> Our nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.[32]

Critical infrastructure networks are overwhelmingly owned and operated by individual private-sector companies; nevertheless, securing these networks is essential to U.S. economic and national security, particularly in view of the emerging threats of nation-state sponsored cyberespionage and cyberwarfare (see *infra* Sections III.B and III.C).

III. THE CHANGING FACE OF CYBERSECURITY: TECHNOLOGY TRENDS

Our nation's cybersecurity challenge is exacerbated by recent technology trends, most notably the: (1) explosive growth in mobile technology; (2) migration to cloud computing; and (3) pervasiveness of social networks.

A. Mobile Technology

Mobile technology continues to penetrate the global market, with the number of mobile devices expected to exceed the number of people on Earth by the end of 2016.[33] At the beginning of 2012, there already were nearly six billion mobile-cellular subscriptions (eighty-six percent "global

32. *National Strategy to Secure Cyberspace*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/national-strategy-secure-cyberspace (last visited Mar. 27, 2013). A prescient report from 1991 similarly described the risks of relying on information technology in a way that continues to resonate today. *See* NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 7 (1991) ("We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.").

33. CISCO, CISCO VISUAL NETWORKING INDEX: CISCO GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2011–2016 3 (2013), http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI-Forecast_QA.pdf.

penetration") and more than one billion mobile-broadband subscriptions worldwide,[34] with the latter figure expected to jump to nearly five billion in 2016.[35] Simultaneously, the global mobile application market is exploding. While it accounted for just $1.7 billion in revenue globally in 2010,[36] it is expected to exceed $30 billion in revenue by the end of 2012[37] and reach $38 billion by 2015.[38] Apple's App Store and Google's Play Store each now offers 700,000 mobile applications for their respective platforms, iOS and Android OS.[39]

"Bring your own device," or "BYOD," is another important trend that has come with the penetration of mobile-broadband. Just a few years ago, Research-in-Motion's ("RIM") Blackberry device was the dominant player in the U.S. smartphone market, but new offerings from Apple, Google, and Microsoft have changed that, with consumers increasingly opting to purchase non-Blackberry devices.[40] For security reasons, it was once

34. *Key Statistical Highlights: ITU Data Release June 2012*, ITU WORLD TELECOMMS. (June 2012), http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf. As mobile penetration increases, the mobile advertising market is expected to continue on its own upward trajectory. Google alone earned $2.5 billion in mobile advertising revenue in 2011, and the mobile advertising market as a whole is expected to grow to $4.4 billion in the United States in 2013, with Facebook and Twitter projected to earn $72.7 million and $129.7 million in mobile advertising revenue, respectively, in 2012. *See* Rachel King, *Google's $8 Billion Mobile Ad Run Rate: The Fine Print*, ZDNET (Oct. 18, 2012, 9:12 PM), http://www.zdnet.com/googles-8-billion-mobile-ad-run-rate-the-fine-print-7000006019/ (explaining that the comparison between Google's $2.5 billion mobile advertising run rate for 2011 at the end of the third quarter and its projected $8 billion run rate for 2012 is "a bit like comparing apples and oranges" because the 2011 rate included "gross revenue from mobile ads" while the 2012 rate also includes "gross revenue from the mobile sales of Google Play content" and from "consumer spending on the Play apps"); Cotton Delo, *Facebook Tests Mobile-Ad Network, Challenging Google and Apple*, ADVERTISING AGE (Sept. 18, 2012), http://adage.com/article/digital/facebook-tests-mobile-ad-network-challenging-google-apple/237279/.

35. Press Release, Ericsson, Ericsson Predicts Mobile Data Traffic to Increase 10-Fold by 2016 (Nov. 7, 2011), http://hugin.info/1061/R/1561267/483146.pdf (predicting that mobile broadband subscriptions will reach nearly five billion in 2016, representing sixty percent year-on-year growth).

36. Austin Carr, *Report: Apps to Explode to $38 Billion Market by 2015*, FAST COMPANY (Mar. 1, 2011, 8:22 AM), http://www.fastcompany.com/1732635/apps-explode-38-billion-market-2015.

37. *Cumulative Mobile App Revenues Set to Exceed $30 Billion by End—2012*, ABI RESEARCH (Nov. 23, 2012), http://www.abiresearch.com/press/cumulative-mobile-app-revenues-set-to-exceed-30-bi.

38. Aemon Malone, *Report: Apps to Become $38 Billion Industry by 2015*, DIGITAL TRENDS (Mar. 1, 2011), http://www.digitaltrends.com/mobile/report-apps-to-become-38-billion-industry-by-2015/.

39. Damien Scott, *Google Play Store Now Has as Many Apps as Apple App Store*, COMPLEX (Oct. 30, 2012, 1:57 PM), http://www.complex.com/tech/2012/10/google-play-store-now-has-as-many-apps-as-apple-app-store.

40. In 2010, Research-in-Motion, which created the Blackberry, had thirty-nine

typical for U.S. corporations to require their employees to access corporate networks using only corporate-issued devices (typically BlackBerry devices, which earned top marks for enterprise security and was number one in the U.S. smartphone market).[41] Today's corporations increasingly permit employees to use mobile devices of their own choosing, including those offered by Apple (e.g., iPhone, iPad), Google (e.g., Android devices), and Microsoft.[42] Demand for the convenience and productivity offered by these devices may have started in corporate boardrooms, but it quickly trickled down to the rest of the corporate workforce and has put substantial pressure on corporations to loosen their previously restrictive corporate policies.

Mobile technology, by itself, poses a tremendous cybersecurity challenge. Smartphones equipped with internal microphones, cameras, and geolocation may be "the ultimate spy tool,"[43] enabling hackers to listen to calls made on the device, monitor text messages to and from the device, and track the location of the device.[44] Hackers could use a hacked phone

---

percent of the U.S. smartphone market. Today, it has just 9.5%. David Goldman, *BlackBerry's Wipeout Creates Major Mobile Security Gaps*, CNN MONEY (Sept. 26, 2012, 7:25 AM), http://money.cnn.com/2012/09/26/technology/mobile-security-byod/index.html.

41. *Id.*

42. Debra Cassens Weiss, *Bye-Bye BlackBerrys: 88% of BigLaw CIOs Expect Use to Decline in Next Year*, A.B.A. J. (Nov. 7, 2012, 5:30 AM), http://www.abajournal.com/news/article/bye-bye_blackberrys_88_of_large_firm_cios_expect_use_to_decline_in_next_yea (reporting that an *American Lawyer* survey of eighty-three Chief Information Officers ("CIOs") and technology chiefs at the nation's top law firms found that "eighty-eight percent of the CIOs expect a net drop in the number of BlackBerry users at their law firms in the next twelve months"). Apple's iPhone is reported to have roughly matched RIM's BlackBerry devices when it comes to enterprise security. Nick Heath, *iPhone Now as Secure as BlackBerry, Say Tech Chiefs*, TECHREPUBLIC (Sept. 18, 2012, 3:39 AM), http://www.techrepublic.com/blog/cio-insights/iphone-now-as-secure-as-blackberry-say-tech-chiefs/39749386.

43. Darlene Storm, *Mobile RAT Attack Makes Android the Ultimate Spy Tool*, COMPUTERWORLD (Mar. 1, 2012, 11:50 AM), http://blogs.computerworld.com/19803/mobile_rat_attack_makes_android_the_ultimate_spy_tool (quoting George Kurtz, former Chief Technology Officer of McAfee Labs); *see Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise*, FBI (Oct. 12, 2012), http://www.fbi.gov/scams-safety/e-scams (warning smartphone users regarding vulnerabilities in Android devices and suggesting preventative measures).

44. *See* Ken Dilanian, *New Security Flaw Discovered in Smartphones*, L.A. TIMES (Feb. 24, 2012), http://articles.latimes.com/2012/feb/24/business/la-fi-smartphone-hacking-20120224 ("[A cybersecurity researcher successfully] used a previously unknown hole in smartphone browsers to plant China-based malware that can commandeer the device, record its calls, pinpoint its location and access user texts and emails."). At the annual RSA Conference, security researchers recently offered a live demonstration of their successful "remote-access-tool" attack on an Android phone that

"as a hidden camera, secretly record video, tap into the microphone to eavesdrop or make audio recordings, and track your movements via GPS location."[45] Moreover, physical control over mobile devices is easily compromised due to their small size and portability,[46] and built-in security mechanisms are often unused[47] or easily circumvented, facilitating unauthorized third-party control over mobile devices.[48] Moreover, as devices become more functional, they often become less secure simply because there are more ways to introduce vulnerabilities: "Every app you install on your mobile device could lead to compromise, every text message you receive. Every website you browse using your own device's mobile browser is possibly suspect."[49]

In the BYOD environment, securing mobile devices is even more important. An employee's compromised device could be used to "listen in to business meetings for espionage or for insider trading"[50] or could serve as a "back door" into corporate networks.[51] Moreover, "[i]f just one device has been compromised—if a single employee clicks on a bad link, downloads a malicious app, or leaves the device at a bar—attackers could get a free pass into the network."[52] Corporations embracing the BYOD phenomenon may be "offering up a way into their networks on a silver platter."[53]

---

enabled them to activate the smartphone's microphone to listen to calls made on the device, monitor text messages to and from the targeted smartphone, and track the location of the device. CrowdStrike, *RSA 2012-Hacking Exposed: Mobile RATs (CrowdStrike)*, YOUTUBE (Mar. 4, 2012), http://www.youtube.com/watch?v=9smxU4gu8ac.

45. Storm, *supra* note 43.

46. WAYNE JANSEN & TIMOTHY GRANCE, NAT'L INST. OF SCIENCE AND TECH., GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING, SPECIAL PUBLICATION 800-144 viii (2011), http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

47. *Id.*; *see* Goldman, *supra* note 40 (reporting results of a Ponemon Institute study finding that fifty-nine percent of corporations that allow BYOD report that their employees fail to lock their personal devices, and fifty-one percent experienced some form of data loss as a result).

48. JANSEN & GRANCE, *supra* note 46, at viii.

49. Goldman, *supra* note 40.

50. Storm, *supra* note 43.

51. *See* Patrick Lambert, *BYOD: Risks, Rewards, and How to Deal with It*, TECHREPUBLIC (Nov. 1, 2012, 9:00 AM), http://www.techrepublic.com/blog/security/byod-risks-rewards-and-how-to-deal-with-it/8622 (noting the risk that an employee could bring an infected laptop that could open a back door into a network).

52. Goldman, *supra* note 40.

53. *Id.*

B. Cloud Computing[54]

Another important technology trend is the migration to cloud computing. Cloud computing is constantly evolving,[55] leading to some confusion over the precise contours of the term,[56] but "at the most basic level, cloud computing means that your data is stored on somebody else's computer."[57] It is generally agreed that cloud computing refers to delivering computing resources as a service over a network.[58] Cloud computing has been

54. The National Institute of Standards and Technology ("NIST") defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," but cautions that "[c]loud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation." PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF SCIENCE AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING, SPECIAL PUBLICATION 800-145 1–2 (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. The NIST definition was the result of four years of work and fifteen draft definitions. *Final Version of NIST Cloud Computing Definition Published*, NIST (Oct. 25, 2011), http://www.nist.gov/itl/csd/cloud-102511.cfm. There are a number of competing theories regarding the origin of the term "cloud computing." Some assert that the term comes from "the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams." *See, e.g.*, Lakhmi Chand Goyal & Pradeep Kumar Jatav, *Cloud Computing: An Overview and Its Impact on Libraries*, 1 INT'L J. OF NEXT GENERATION COMPUTER APPLICATIONS 9, 9 (2012), http://ijngca.com/Papers/IJNGCA08092012.pdf. Others disagree. *See, e.g.*, John Willis, *Who Coined the Phrase Cloud Computing?*, IT MGMT. & CLOUD BLOG (Dec. 31, 2008), http://www.johnmwillis.com/cloud-computing/who-coined-the-phrase-cloud-computing/ (listing three different possibilities for the origins of the phrase).

55. Arif Mohamed, *A History of Cloud Computing*, COMPUTERWEEKLY (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing ("Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS)."); *What Is The Cloud?*, GEN. SERVS. ADMIN., http://www.info.apps.gov/content/what-cloud (last visited Mar. 27, 2013) (discussing the evolution of today's cloud computing from grid and utility computing).

56. *Most Americans Confused by Cloud Computing According to National Survey*, CITRIX (Aug. 28, 2012), http://www.citrix.com/lang/English/lp/lp2328330.asp (reporting that most respondents in a recent survey believed the cloud is related to weather and that ninety-five percent of respondents who thought they were not using the cloud actually were).

57. *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 13 (2010) [hereinafter *ECPA Reform Hearing*] (statement of Edward W. Felten, Professor, Princeton University), http://judiciary.house.gov/hearings/printers/111th/111-149_58409.pdf.

58. *See, e.g., Computing: Services Overview*, ACCENTURE,

analogized to the modern high-rise office building: "[j]ust as a high-rise allows tenants to lease secure, individual offices in the same building while sharing core services such as plumbing and electricity, multi-tenant enterprise cloud computing allows organizations to use individualized software applications while sharing core computing services such as database and security."[59]

The reported benefits of cloud computing include scalability,[60] rapid deployment,[61] greater reliability,[62] efficiency,[63] increased storage,[64] flexibility,[65] business agility,[66] cost savings,[67] and energy savings.[68]

---

http://www.accenture.com/sk-sk/Pages/service-technology-cloud-computing-overview-summary.aspx (last visited Mar. 27, 2013) (defining cloud computing as "the dynamic provisioning of IT capabilities (hardware, software, or services) from third parties over a network"); *see also* Mohamed, *supra* note 55 ("The idea of an 'intergalactic computer network' was introduced in the sixties by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) [the predecessor to today's Internet] in 1969.").

59. *ECPA Reform Hearing*, *supra* note 57, at 44 (statement of David Schellhase, Executive Vice President & General Counsel, Salesforce.com).

60. *See ECPA Reform Hearing*, *supra* note 57, at 14 (statement of Edward W. Felten, Professor, Princeton University) ("[I]f [a] start-up's business grows rapidly and it needs to expand its computing capacity dramatically to handle a flood of new customers, this is easily done in the cloud, by simply increasing the number of servers the start-up is renting from the provider."); Andrew Nusca, *The Future of Cloud Computing: 9 Trends for 2012*, ZDNET (June 21, 2012, 3:26 AM), http://www.zdnet.com/blog/btl/the-future-of-cloud-computing-9-trends-for-2012/80511 (reporting that "scalability is driving adoption," with fifty-seven percent of companies in a recent poll identifying scalability as the most important reason they switched to the cloud).

61. MELL & GRANCE, *supra* note 54, at 2.

62. *See ECPA Reform Hearing*, *supra* note 57, at 14 (statement of Edward W. Felten, Professor, Princeton University).

63. *Id.* at 44 (statement of David Schellhase, Executive Vice President & General Counsel, Salesforce.com) ("By eliminating the need for costly and wastefully duplicative infrastructure, multi-tenant cloud computing frees users to focus on their core business, not their IT.").

64. Mohamed, *supra* note 55 (" 'Many IT professionals recognise the benefits cloud computing offers in terms of increased storage, flexibility and cost reduction,' said Songian Zhou, chief executive officer of *Platform Computing*.").

65. Rajani Baburajan, *The Rising Cloud Storage Market Opportunity Strengthens Vendors*, TMCNET (Aug. 24, 2011), http://technews.tmcnet.com/channels/cloud-storage/articles/211183-rising-cloud-storage-market-opportunity-strengthens-vendors.htm ("Cloud computing is becoming the preferred choice of organizations not only because of its cost savings but also because of the flexibility.").

66. *See id.* (observing that cloud computing enables enterprises to add capacity on demand).

67. *See id.*

68. Katie Fehrenbacher, *Cloud Computing Could Lead to Billions in Energy Savings*, GIGAOM (July 21, 2011, 8:48 AM), http://gigaom.com/2011/07/21/cloud-computing-could-lead-to-billions-in-energy-savings/ (reporting that cloud computing

By any measure, the market for cloud computing services is exploding. Global cloud computing revenue is projected to grow at a compound annual growth rate of 28.8% between now and 2015, and the market is expected to increase from $46 billion in 2009 to over $210 billion by 2015, according to analysts.[69]

Despite this rapid growth, many corporations are reluctant to embrace cloud-based solutions due to security concerns.[70] In a recent poll, more than half of the companies surveyed identified security as the reason that they have not adopted cloud computing technology.[71]

From a corporate cybersecurity perspective, the public cloud is a double-edged sword. It offers a number of potential benefits, including professionally managed security,[72] backup and recovery capabilities,[73] and

---

could lead to an estimated $12.3 billion in energy savings and 85.7 million metric tons of carbon emissions savings per year by 2020, according to AT&T-sponsored research); *id.* ("[M]oving business applications to the cloud could cut the associated per-user carbon footprint by 30 percent for large, already-efficient companies and as much as 90 percent for the smallest and least efficient businesses."); *see* Press Release, Pike Research, Cloud Computing to Reduce Global Data Center Energy Expenditures by 38% in 2020 (Dec. 6, 2010), *available at* http://www.pikeresearch.com/newsroom/cloud-computing-to-reduce-global-data-center-energy-expenditures-by-38-in-2020 (forecasting that cloud computing could lead to a thirty-eight percent reduction in worldwide data center energy use by 2020 due to substantial energy efficiency benefits); *Cloud Computing Energy Efficiency: Strategic and Tactical Assessment of Energy Savings and Carbon Emissions Reduction Opportunities for Data Centers Utilizing SaaS, IaaS, and PaaS,* NAVIGANT RES., http://www.pikeresearch.com/research/cloud-computing-energy-efficiency (last visited Mar. 27, 2013) ("[W]e anticipate that much of the work done today in internal data centers will be outsourced to the cloud by 2020, resulting in significant reductions in energy consumption, associated energy expenses, and GHG emissions from data center operations versus a business as usual (BAU) scenario.").

69. *Cloud Computing Energy Efficiency*, *supra* note 68; Press Release, Gartner, Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010 (June 22, 2010), *available at* http://www.gartner.com/it/page.jsp?id=1389313 (reporting that the worldwide market for cloud services will be worth $148.8 billion by 2014); *accord*, Louis Columbus, *Gartner Predicts Infrastructure Services Will Accelerate Cloud Computing Growth*, FORBES, (Feb. 19, 2013, 12:36 PM), http://www.forbes.com/sites/louiscolumbus/2013/02/19/gartner-predicts-infrastructure-services-will-accelerate-cloud-computing-growth/ (reporting that global spending on public cloud services is expected to achieve a compound annual growth rate of 17.7% from 2011 through 2016 and that the worldwide market for cloud services is expected to grown from $76.9 billion in 2010 to $210 billion in 2016).

70. Robert Scheier, *Cloud Computing Tools: Improving Security Through Visibility and Automation*, CSO ONLINE (May 14, 2012), http://www.csoonline.com/article/706357/cloud-computing-tools-improving-security-through-visibility-and-automation.

71. Nusca, *supra* note 60 (reporting the results of a North Bridge Venture Partners poll of 785 people at thirty-nine enterprise technology companies, which noted a concern regarding regulatory compliance and vendor lock-in as additional reasons for inhibition of adoption of cloud-computing).

72. *ECPA Reform Hearing*, *supra* note 57, at 13 (statement of Edward W. Felten, Professor, Princeton Univ.). Cloud provider reliance on "dedicated personnel" to

automation of vulnerability mitigation and security management functions[74] (although automation may be prohibitively expensive for many companies[75]). But other characteristics of cloud computing—including system complexity,[76] the multi-tenant environment,[77] and loss of control[78]—pose significant challenges to corporate cybersecurity.[79]

---

maintain security, manage software updates, and "continually strengthen" security measures could boost corporate security. *Advancements in Cloud Security*, DLT SOLUTIONS, http://www.dlt.com/technology/cloud-computing/understanding-cloud-computing/cloud-security/advancements-in-cloud-securi (last visited Mar. 27, 2013). Indeed, "[c]loud providers . . . have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Increases in the scale of computing induce specialization, which in turn allows security staff to shed other duties and concentrate exclusively on security issues. Through increased specialization, there is an opportunity for staff members to gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties." JANSEN & GRANCE, *supra* note 46, at 9.

73. JANSEN & GRANCE, *supra* note 46, at 9–10. ("Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when faced with increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents.").

74. 3rdID8487, *Cyber Security and American Power*, YOUTUBE, at 34:30 (July 11, 2012), http://www.youtube.com/watch?v=nTwiZneMw3U [hereinafter *Keith Alexander's Remarks*]. JANSEN & GRANCE, *supra* note 46, at 9 ("Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities [such as] configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also profit from a uniform, homogeneous cloud infrastructure . . . ."); Scheier, *supra* note 70 ("[T]he same automated, consistent provisioning that is essential to managing either public or private clouds . . . can also offer the fringe benefit of improving security . . . . Because so many security vulnerabilities are caused by human error, automating proper server configuration also automatically improves security . . . . Automated server provisioning tools . . . help prevent variations that could create vulnerabilities . . . . [and] enable administrators to easily control common security-sensitive settings, such as which ports are open and which services are running.").

75. Scheier, *supra* note 70 ("[H]igh [per server] costs force organizations with thousands of servers to go without automated patch or configuration management or audit compliance . . . relying instead on scripts or manual processes.").

76. JANSEN & GRANCE, *supra* note 46, at 10–11 ("Many components make up a public cloud, resulting in a large attack surface . . . . Security depends not only on the correctness and effectiveness of many components, but also on the interactions among them.").

77. *Id.* at 11 ("Having to share an infrastructure with unknown outside parties can be a major drawback for some applications . . . .").

78. *Id.* at 12 ("Loss of control over both the physical and logical aspects of the system and data diminishes the organization's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security . . . that are in the best interest of the organization.").

79. *See generally id.*; *see also* Jon Brodkin, *Gartner: Seven Cloud-Computing*

Moreover, many cloud characteristics themselves are double-edged swords. Take data concentration, for example. Concentrating data in the cloud may expose data to fewer risks than a more distributed model in which data resides on mobile devices, laptops, or other peripherals that can be lost or stolen. However, consolidating data in one location creates an attractive target and could render a successful security breach disastrous.[80] Likewise, a uniform cloud infrastructure may benefit information assurance activities, but may enable "a single flaw [to] manifest[] throughout the cloud, potentially impacting all tenants and services."[81]

C. Social Networking

The rise of social networking also brings new cybersecurity challenges. Hackers have long relied on "social engineering"—convincing people to disclose information that they should not[82]—to gain the trust of targets and compromise their networks. Now, detailed information gleaned from social networking sites is helping adversaries successfully target even the most sophisticated corporate victims through social engineering.[83]

The May 2011 attack on RSA Security ("RSA"), one of the nation's oldest and best-known security technology companies, serves as a cautionary tale regarding how adversaries use social engineering to compromise their victims' networks. In RSA's case, a spear-phishing email (i.e., an email used to "target specific people at enterprises with the aim of gaining a foothold into the corporate network"[84]) was sent to two

---

Security Risks, INFOWORLD (July 2, 2008), http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

80. Mathew J. Schwartz, *Epsilon Fell to Spear-Phishing Attack*, INFORMATIONWEEK (Apr. 11, 2011, 3:55 PM), http://www.informationweek.com/security/attacks/epsilon-fell-to-spear-phishing-attack/229401372 ("The Epsilon breach highlights that with the growth of cloud services, one data breach can be a single point of failure for numerous organizations . . . . [E]ntrusting a single company with data on so many people makes it an attractive target for attackers, which may in fact place customers at greater risk of having their personal information stolen.").

81. JANSEN & GRANCE, *supra* note 46, at 9.

82. Matthew Weinschenk, *CyberSecurity's Biggest Threat is Decidedly Low Tech*, WALL ST. DAILY (Mar. 8, 2012), http://www.wallstreetdaily.com/2012/03/08/cyber-securitys-biggest-threat/.

83. JANSEN & GRANCE, *supra* note 46, at viii ("The growing availability and use of social media, personal Webmail, and other publicly available sites are a concern, since they increasingly serve as avenues for social engineering attacks that can negatively impact the security of the client, its underlying platform, and cloud services accessed.").

84. Robert Westervelt, *Study Finds Spear Phishing at Heart of Most Targeted Attacks*, SEARCHSECURITY (Nov. 29, 2012), http://searchsecurity.techtarget.com/news/2240173534/Study-finds-spear-phishing-at-heart-of-most-targeted-attacks; TRENDMICRO INC., SPEAR-PHISHING EMAIL: MOST FAVORED ATTACK BAIT 1–2 (2012), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-

groups of RSA employees. The subject of the email message was "2011 Recruitment Plan." Attached to the email was a malware-embedded[85] Excel spreadsheet innocuously entitled "2011 Recruitment plan.xls."[86] Although RSA's systems automatically identified and marked the email as "junk," one employee opened the email, thereby unwittingly releasing the malware that ultimately facilitated the exfiltration of sensitive data.[87]

Spear-phishing also was the *modus operandi* in the 2011 attack on Epsilon, an email marketing behemoth. In that attack, an estimated sixty million email addresses were compromised, resulting in an estimated $225 million in costs to Epsilon from the data breach alone.[88] Phishers could

---

papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf ("In a typical spear-phishing attack, a specially crafted email is sent to specific individuals from a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a malware- or an exploit-laden site . . . . [This] installs a malware in a compromised computer. The malware then accesses a malicious command-and-control (C&C) server to await instructions from a remote user. At the same time, [the malware] usually drops a decoy document that will open when the malware or exploit runs to hide malicious activity."). *Id.* at 1 ("[S]pear phishing makes use of information about a target to make attacks more specific and 'personal' to the target. Spear-phishing emails, for instance, may refer to their targets by their specific name, rank, or position instead of using generic titles as in broader phishing campaigns."). A paradigmatic example of spear-phishing came to light as a result of the long-running cyberbattle between the nation-states of Georgia and Russia. In this intriguing case, a Russian hacker believed to be seeking sensitive Georgian government documents on behalf of Russian intelligence "sent a series of emails to [Georgian] government officials that appeared to come from the president of Georgia, with the address 'admin@president.gov.ge.' Those emails contained a malicious PDF attachment, purportedly containing legal information, with an exploit that delivered malware." Jeremy Kirk, *Georgia Outs Russia-Based Hacker—With Photos*, PC WORLD (Oct. 30, 2012, 11:20 AM), http://www.pcworld.com/article/2013289/georgia-outs-russia-based-hacker-with-photos.html.

85. *Malware (Malicious Software)*, SEARCHMIDMARKETSECURITY, http://searchmidmarketsecurity.techtarget.com/definition/malware (last updated Oct. 2008) ("Malware . . . is any program or file that is harmful to a computer user.").

86. Peter Bright, *Spearphishing + Zero-Day: RSA Hack* Not *"Extremely Sophisticated,"* ARS TECHNICA, (Apr. 4, 2011, 4:17 PM), http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/.

87. Opening the email attachment led to installation of a variant of the Poison Ivy RAT. A RAT is "a Remote Administration/Access Tool/Toolkit/Trojan. RATs allow remote access to files, the registry, monitoring of network access, starting and stopping programs, and more, making them extremely powerful: anything the user can do locally, the hacker can do remotely . . . . With Poison Ivy installed, the attacker stole user credentials and escalated their privileges to gain access to secure systems that the originally compromised user didn't have access to. The attacker then used this system access to exfiltrate . . . sensitive data . . . ." *Id.*

88. *Total Cost of Epsilon E-mail Breach Could Reach $225M, Including up to $45M in Lost Business, According to New Report by CyberFactors*, BUS. WIRE (Apr. 29, 2011, 12:29 PM), http://www.businesswire.com/news/home/20110429005630/en/Total-Cost-Epsilon-E-Mail-Data-Breach-Reach.

further exploit the compromised email addresses, leading some to project that the Epsilon breach could generate up to $4 billion in total costs, including fines, litigation, lost business, forensic audits, and monitoring.[89]

As corporate security improves, adversaries increasingly rely on "social engineering" to gain the trust of targets, to convince people to disclose information that they should not,[90] and subsequently to compromise targets' networks. Thirty-seven percent of records compromised through cyber data breaches were compromised as a result of incidents employing social tactics.[91] Moreover, industry data suggest that spear-phishing is at the heart of most targeted attacks.[92]

Government and private sector cybersecurity experts warn that hackers increasingly are exploiting information gleaned from social networking sites for social engineering-based attacks. For example, the FBI warns that "[p]redators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation."[93] Security provider Trend Micro warns:

> While human-related information like a target's name, job title, and email address may be bought from the underground market or be provided by the masterminds behind sanctioned attacks, the Internet is the most convenient source of such information. Social networking sites, corporate and academic publications, and organizations' sites allow miscreants to harvest relevant information on their targets for various social engineering schemes.[94]

Indeed, "[e]lite cybercriminals are tapping into search engines and social networks to help them target specific employees for social-engineering trickery at a wide range of companies, professional firms and government agencies."[95]

---

89. *Id.*

90. Weinschenk, *supra* note 82.

91. VERIZON, VERIZON'S 2012 DATA BREACH INVESTIGATIONS REPORT 33 (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

92. Ninety-one percent of targeted attacks involved spear-phishing, and ninety-four percent of emails contained malicious file attachments, according to TrendMicro's analysis of targeted attack data collected between February and September of 2012. *See* TRENDMICRO INC., *supra* note 84, at 1.

93. FBI, U.S. DEP'T OF JUSTICE, INTERNET SOCIAL NETWORKING RISKS 2, http://www.ncix.gov/issues/cyber/internet-social-networking-risks.pdf.

94. TRENDMICRO INC., *supra* note 84, at 5.

95. Byron Acohido, *Social-Media Tools Used to Target Corporate Secrets*, USA TODAY (Mar. 31, 2011), http://usatoday30.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm ("[M]any attacks [that cybersecurity firm] Mandiant has investigated began with the criminals doing reconnaissance on Google, Facebook, LinkedIn, Twitter and other popular Internet services to find companies to

IV. THE CHANGING FACE OF CYBERSECURITY: CYBERTHREAT TRENDS

There are only two types of companies in this country: those who know they have been hacked, and those who don't.[96]

Cybercrime,[97] cyberespionage,[98] and cyberwarfare[99] have long been understood to threaten the security of cyberspace, however the gravity of the cyberthreat recently has been publicly underscored with increasing frequency at the highest levels of the United States government. President Obama penned a *Wall Street Journal* op-ed in August 2012 describing the cyberthreat as "one of the most serious economic and national security challenges" facing our nation.[100] Six months later, he emphasized the importance of cybersecurity in his post-election State of the Union address,

---

target—and pinpoint specific executives, researchers, analysts, engineers or key administrative assistants to attack. The next step is to craft a spear-phishing lure designed to entice a specific employee to click on a viral attachment or Web page link, using information gleaned during the reconnaissance phase to make the attachment or link seem trustworthy.").

96. Although the precise origin of this statement appears to be unknown, it is used quite frequently in cybersecurity circles. *See, e.g.*, DMITRI ALPEROVITCH, MCAFEE, REVEALED: OPERATION SHADY RAT 2 (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf ("I divide the entire set of Fortune Global 2,000 firms into two categories: those that *know they've been compromised*, and those that *don't yet know*.") (emphasis in original); Jonathan Fisher, *China Has Hacked Every U.S. Major Company, Claims Richard Clarke*, WEBPRONEWS (Mar. 28, 2012), http://www.webpronews.com/china-has-hacked-every-u-s-major-company-claims-richard-clarke-2012-03 (" 'There are two kinds of companies: those that have been hacked, and those that will be.' If you listen to people talk about cyber security long enough, you'll hear a hundred subtle variations of that statement. Another version goes: 'There are two kinds of companies: those that know they've been hacked, and those that don't,' implying that every server and every computer the world over is not only vulnerable to attack, but has at least been probed in the past.").

97. *See, e.g.*, Meredith Johnston, *Cybercrime is on the rise*, TECHREPUBLIC (June 16, 2000, 7:00 AM), http://www.techrepublic.com/article/cybercrime-is-on-the-rise/5032146 (illustrating twelve types of cybercrime, including financial fraud, denial of service, and theft of proprietary information).

98. *See, e.g.*, Nathan Thornburg, *Inside the Chinese Hack Attack*, TIME (Aug. 25, 2005), http://www.time.com/time/nation/article/0,8599,1098371,00.html.

99. *See, e.g.*, John Stanton, *Rules of Cyber War Baffle U.S. Government Agencies*, NAT'L DEF. MAG. (Feb. 2000), http://www.nationaldefensemagazine.org/archive/2000/February/Pages/Rules4391.aspx; *U.S. Army Kick-Starts Cyber War Machine*, CNN (Nov. 22, 2000), http://articles.cnn.com/2000-11-22/tech/cyberwar.machine.idg_1_computer-viruses-denial-of-service-cyberwarfare?_s=PM:TECH.

100. Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

declaring: "America must . . . face the rapidly growing threat."[101] In March 2013, just one year after FBI Director Robert Mueller warned that cyberthreats were expected to surpass terrorism as the single "greatest threat" to the United States,[102] the U.S. Director of National Intelligence ("DNI") publicly identified cyber as the top global threat facing America, stating "it's hard to overemphasize its significance."[103] The next day, President Obama invited select CEOs of critical infrastructure companies directly to the White House to discuss cybersecurity,[104] and a few weeks later, in April 2013, he "summoned 15 of America's top financial leaders to the White House to discuss . . . cyberrisks."[105]

Throughout 2012, other top national security officials also publicly emphasized the gravity of the cyberthreat. In February 2012, former Director of the National Security Agency ("NSA") and former DNI, Mike McConnell, said: "The United States is fighting a cyberwar today, and we are losing."[106] In October 2012, then-Defense Secretary Leon Panetta warned that the United States is at risk for a "cyber Pearl Harbor,"[107] saying

---

101. Barack Obama, Remarks by the President in the State of the Union Address (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address. The President took the opportunity afforded by his State of the Union address to signal his intention to make cybersecurity a priority in his second term and to lay out his plan for doing so, stating: "Earlier today, I signed a new executive order that will strengthen our cyber defenses . . . . But now Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks. This is something we should be able to get done on a bipartisan basis." *Id.*

102. Stacy Cowley, *FBI Director: Cyberthreat will eclipse terrorism*, CNN MONEY, (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm (quoting FBI Director Mueller saying: "Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country").

103. *Worldwide Threat Assessment: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 5–6 (2013) (remarks by James R. Clapper, Director of Nat'l Intelligence), http://www.dni.gov/files/documents/Intelligence%20Reports/WWTA%20Remarks%20as%20delivered%2012%20Mar%202013.pdf.

104. Alex Mooney, *President to Host CEOs in Situation Room for Cyber Security Chat*, CNN (Mar. 13, 2013, 1:22 PM), http://security.blogs.cnn.com/2013/03/13/president-to-host-ceos-in-situation-room-for-cyber-security-chat/.

105. Frederick Kempe, *Seeking to Avert Cyberwar*, April 15, 2013. http://blogs.reuters.com/thinking-global/2013/04/15/seeking-to-avert-cyber-war/. An executive who participated in the April meeting explained: "[t]he President scared the hell out of all of us, and we're not easy to frighten." *Id.*

106. Mike McConnell, *Mike McConnell on How to Win the Cyber-War We're Losing*, WASH. POST (Feb. 28, 2012), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493pf.html.

107. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on US*, N.Y. TIMES (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

"[t]his is a pre—9/11 moment."[108] Finally, with respect to cyberespionage, Richard Clarke, former counterterrorism czar in the Clinton and both Bush administrations, warned of an impending "death of a thousand cuts [whereby] we lose our competitiveness by having all of our research and development stolen by the Chinese."[109]

Whatever one may think of the merits of these claims,[110] it is clear that despite corporate America's increasing awareness of, and investment in, cybersecurity, our digital assets and infrastructure routinely are being exploited. U.S. victims of major cyberincidents[111] over the past few years

---

108. Julian E. Barnes & Siobhan Gorman, *U.S. Readies Cyberdefense*, WALL ST. J. (Oct. 11, 2012, 10:29 PM), http://online.wsj.com/article /SB10000872396390444657804578051071681887566.html.

109. Emil Protalinski, *Richard Clarke: China Has Hacked Every Major US Company*, ZDNET (Mar. 27, 2012, 6:04 AM), http://www.zdnet.com/blog/security /richard-clarke-china-has-hacked-every-major-us-company/11125.

110. Bruce Schneier, *The Threat of Cyberwar Has Been Grossly Exaggerated*, SCHNEIER ON SECURITY (July 7, 2010, 12:58 PM), http://www.schneier.com/blog /archives/2010/07/the_threat_of_c.html ("[T]he entire national debate on cyberwar is plagued with exaggerations and hyperbole."); Maggie Shiels, *Cyber War Threat Exaggerated Claims Security Expert*, BBC (last updated Feb. 16, 2011, 4:21 AM), http://www.bbc.co.uk/news/technology-12473809 (reporting on claims that the threat of cyberwar is greatly exaggerated and quoting security expert Bruce Schneier, who said that, instead of cyberwar, "we are seeing . . . an increasing use of war-like tactics and that is what is confusing us"); Barnes & Gorman, *supra* note 108 (explaining that, according to one expert, then-Secretary Panetta's remarks "described the gravest attack Americans might face, not the most likely," and that the 9/11 tragedy in which over 3,000 people died is "an unlikely scenario for a cyberthreat . . . in the near term").

111. Although this Article focuses on the United States, other countries are not immune from cyberexploitation, as recent breaches involving foreign aerospace, defense, and manufacturing industries illustrate. *See, e.g.*, *Japan Confesses Data Breach on Epsilon Rocket*, VOICE OF RUSSIA (Dec. 3, 2012, 2:04 PM), http://english.ruvr.ru/2012_11_30/Japan-confesses-data-breach-on-Epsilon-rocket/ (describing a recent breach at the Japan Aerospace Exploration Agency ("JAXA") that resulted in exfiltration of sensitive data about Japan's rocket program, including the "parameters" and "specifics of engine maintenance" for Japan's solid-fueled Epsilon Rocket). Notably, solid-fuel rockets of Epsilon's size can be used as intercontinental ballistic missiles. *See also* Matteo Emanuello, *Epsilon Rocket Data Stolen by Hackers*, SPACE SAFETY MAGAZINE (Dec. 5, 2012, 4:36), http://www.spacesafetymagazine.com /2012/12/05/epsilon-rocket-data-stolen-hackers/; Nicole Perlroth, *Nissan Is Latest Company to Get Hacked*, N.Y. TIMES BITS BLOG (Apr. 24, 2012, 12:34 PM), http://bits.blogs.nytimes.com/2012/04/24/nissan-is-latest-company-to-get-hacked/ ("Nissan confirmed its computer systems were hacked . . . . The attack is just the latest in a string of cyberattacks on corporations . . . ."); Eric Savitz, *Military Contractor Mitsubishi Heavy Hit by Hack Attack*, FORBES (Sept. 19, 2011, 12:43 PM), http://www.forbes.com/sites/ericsavitz/2011/09/19/military-contractor-mitsubishi-heavy-hit-by-hack-attack/ (describing a "major hack attack" on Mitsubishi Heavy Industries in which data reportedly was exfiltrated from "the Japanese industrial giant that makes submarines, missiles and components for nuclear power plants"). David Leppard, *Chinese Steal Jet Secrets from BAE*, THE SUNDAY TIMES (Mar. 11, 2012), http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article991581.ece ("Chinese spies hacked into computers belonging to BAE Systems, Britain's biggest

include: U.S. Chamber of Commerce (May 2010),[112] Google (June 2010),[113] RSA Security (May 2011),[114] Sony (May 2011; October 2012),[115] Booz Allen Hamilton (July 2011),[116] U.S.-China Economic and Security Review Commission (September 2011),[117] twenty-three natural gas pipeline operators (December 2011–June 2012),[118] Global Payments (March 2012),[119] numerous financial services companies and the New York Stock Exchange (September 2012–March 2013),[120] the White House

---

defence company, to steal details about the design, performance and electronic systems of the West's latest fighter jet . . . prompt[ing] fears that the jet's radar capabilities could have been compromised.").

112. Nicole Perlroth, *Hacked Chamber of Commerce Opposed Cybersecurity Law*, N.Y. TIMES BITS BLOG (Dec. 21, 2011, 6:10 PM), http://bits.blogs.nytimes.com /2011/12/21/hacked-chamber-of-commerce-opposed-cybersecurity-law/ ("The United States Chamber of Commerce has confirmed Chinese hackers last year broke into internal networks.").

113. *See infra* note 158.

114. Riva Richmond, *The RSA Hack: How They Did It*, N.Y. TIMES BITS BLOG (Apr. 2, 2011, 3:17 PM), http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/.

115. Christopher MacManus, *Sony's PlayStation 3 Experiences Its Biggest Hack Yet*, CNET (Oct. 24, 2012, 7:48 PM), http://news.cnet.com/8301-17938_105-57539756-1/sonys-playstation-3-experiences-its-biggest-hack-yet/; Jason Shreier, *Sony Hacked Again; 25 Million Entertainment Users' Info at Risk*, WIRED (May 2, 2011, 7:11 PM), http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack/.

116. Andy Greenberg, *Anonymous Hackers Breach Booz Allen Hamilton, Dump 90,000 Military E-Mail Addresses*, FORBES (July 11, 2011), http://www.forbes.com/sites/andygreenberg/2011/07/11/anonymous-hackers-breach-booz-allen-hamilton-dump-90000-military-email-addresses/.

117. Mark Hosenball, *U.S. Authorities Probe U.S.-China Commission Email Hack*, REUTERS (Jan. 10, 2012, 7:09 AM), http://www.reuters.com/article/2012/01/10/us-usa-india-hacking-idUSTRE80828N20120110 ("U.S. authorities are investigating allegations that an Indian government spy unit hacked into emails of [USCC,] an official U.S. commission that monitors economic and security relations between the United States and China, including cyber-security issues.").

118. Mark Clayton, *Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*, CHRISTIAN SCI. MONITOR (Feb. 27, 2013), http://www.csmonitor.com /Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage.

119. The breach of credit card payment processor Global Payments, Inc. potentially exposed personal information, card numbers, and card-verification codes associated with millions of Visa and MasterCard cardholders. Global Payments estimates that the breach affected at least 1.5 million accounts in North America and cost the company $93.9 million dollars. Info. Sec. Media Grp., *Global Payments Breach Tab: $94 Million*, BANK INFO SEC. (Jan. 10, 2013), http://www.bankinfosecurity.com /global-payments-breach-tab-94-million-a-5415/op-1.

120. Tracy Kitten, *DDoS: 6 Banks Hit On Same Day*, BANK INFO SEC. (Mar. 14, 2013), http://www.bankinfosecurity.com/ddos-6-banks-hit-on-same-day-a-5607 ("Six leading U.S. banking institutions were hit by distributed-denial-of-service attacks on March 12, the largest number of institutions to be targeted in a single day."); Perlroth, *supra* note 112 (describing a massive distributed denial of service attack with

(September 2012),[121] Nationwide Mutual Insurance Company (October 2012),[122] major U.S. media outlets including the New York Times[123] and Wall Street Journal (October 2012–January 2013),[124] the Alabama State Government (January 2013),[125] the U.S. Sentencing Commission (January 2013),[126] the U.S. Probation Office for the Eastern District of Michigan,[127] Evernote (March 2013),[128] and Reddit (April 2013).[129] Large-scale cyberoperations uncovered during the same time period include Red October, an alleged Chinese cyberespionage operation uncovered in October 2012,[130] and a massive operation discovered in early 2013 that

---

"unprecedented" volume of traffic affecting U.S. financial institutions, including Wells Fargo, U.S. Bank, PNC, the New York Stock Exchange, and others).

121. Jana Winter & Jeremy A. Kaplan, *White House Confirms Chinese Hack Attack on White House Computer*, FOX NEWS (Oct. 1, 2012), http://www.foxnews.com/tech/2012/10/01/washington-confirms-chinese-hack-attack-on-white-house-computer/.

122. *Nationwide Insurance Says Data Breach Affects 1.1M*, ASSOCIATED PRESS – THE BIG STORY (Dec. 5, 2012, 4:03 PM), http://bigstory.ap.org/article/nationwide-insurance-says-data-breach-affects-11m.

123. Nicole Perlroth, *Hackers in China Attacked the Times for Last 4 Months*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html.

124. Siobhan Ghorman et al., *Chinese Hackers Hit U.S. Media*, WALL ST. J. (Jan. 31, 2013, 8:28 PM), http://online.wsj.com/article/ SB10001424127887323926104578276202952260718.html ("[The Wall Street Journal's] computer systems had been infiltrated by Chinese hackers, apparently to monitor its China coverage.").

125. Press Release, Office of the Ala. Dep't of Homeland Sec., ALDHS Director Details Cyber Intrusion in State IT System (Jan. 29, 2013), *available at* http://www.homelandsecurity.alabama.gov/news_detail.aspx?ID=7511.

126. Will Oremus, *Aaroz Swartz Protestors Take Over Government Websites, Install Asteroids*, SLATE (Jan. 28, 2013, 10:27 AM), http://www.slate.com /blogs/future_tense/2013/01/28/aaron_swartz_protest_anonymous_hacks_government_websites_installs_asteroids.html ("As part of its ongoing protest of the U.S. government's prosecution of computer programmer and activist Aaron Swartz, [hackers affiliated with the group known as] Anonymous . . . hacked the website of the U.S. Sentencing Commission . . . .").

127. *Id.*

128. Doug Gross, *50 Million Compromised in Evernote Hack*, CNNTECH (Mar. 4, 2013, 4:34 PM), http://www.cnn.com/2013/03/04/tech/web/evernote-hacked/ (publicizing hack of Evernote, an online note-taking and archiving service with 50 million users, in which hackers accessed a variety of user information, including user names, e-mail addresses, and encrypted passwords).

129. Dan Kaplan, *Reddit site downed by DDoS attacks*, SC MAGAZINE (Apr. 19, 2013), http://www.scmagazine.com/reddit-site-downed-by-ddos-attacks/article/289680/.

130. Mathew J. Schwartz, *Operation Red October Attackers Wielded Spear Phishing*, INFORMATIONWEEK (January 18, 2013, 3:06 PM), http://www.informationweek.com/security/attacks/operation-red-october-attackers-wielded/240146621 ("The primary focus of this campaign targets countries in Eastern Europe, former USSR republics, and countries in Central Asia, although victims can be found everywhere, including Western Europe and North America.").

victimized Apple,[131] Facebook,[132] Twitter,[133] Microsoft,[134] and an estimated forty other companies.[135]

A. Cybercrime

The term cybercrime is used to refer both to traditional crimes (e.g., extortion,[136] fraud, forgery, identity theft, and child exploitation) that are committed over electronic networks and information systems as well as to crimes unique to electronic networks (e.g., hacking and denial of service attacks).

1. Costs of Cybercrime

By all measures, cybercrime is flourishing.[137] Symantec's Norton estimates global cybercrime costs at $114 billion annually ($388 billion

131. Jim Finkle & Joseph Menn, *Exclusive: Apple, Macs Hit by Hackers Who Targeted Facebook*, REUTERS (Feb. 19, 2013, 4:50 PM), http://www.reuters.com/article/2013/02/19/us-apple-hackers-idUSBRE91110920130219 ("The breaches described by Apple mark the highest-profile cyber attacks to date on businesses running Mac computers."). The hackers are believed to have used a browser-based Java exploit.

132. Doug Gross, *Eastern European Gang Hacked Apple, Facebook, Twitter*, CNNTECH (Feb. 20, 2013, 12:19 PM), http://www.cnn.com/2013/02/20/tech/web/hacked-apple-facebook-twitter/index.html?iref=allsearch.

133. Mathew Schwartz, *Twitter Pursues Two Factor Authentication After Password Breach*, INFORMATIONWEEK (Feb. 4, 2013, 3:06 PM), http://www.informationweek.com/security/application-security/twitter-pursues-two-factor-authenticatio/240147787 ("[Twitter detected] a security breach affecting an estimated 250,000 of its 250 million users.").

134. *Microsoft Hacked: Intrusion Was 'Similar' to Apple and Facebook Hacks*, HUFFINGTON POST (Feb. 22, 2013), http://www.huffingtonpost.com/2013/02/22/microsoft-hacked-apple-hacked-facebook-hacked_n_2745178.html.

135. Dara Kerr, *Apple, Facebook Hackers Hit Car and Candy Companies, Too*, CNET (Mar. 11, 2013, 5:49 PM), http://news.cnet.com/8301-1009_3-57573720-83/apple-facebook-hackers-hit-car-and-candy-companies-too/?utm_medium=twitter ("At least some of these hacks are thought to have originated in Eastern Europe while others are suspected to have come from China. It is unclear if all of the companies were targeted by one group of hackers or if they were isolated incidents.").

136. *See, e.g.*, GAVIN O'GORMAN & GEOFF MCDONALD, SYMANTEC RANSOMWARE: A GROWING MENACE 1–2, http://www.symantec.com/content/en/us/enterprise/media/securityresponse/whitepapers/ransomware-a-growing-menace.pdf (describing ransomware—i.e., malware that locks a target's computer and requires payment of a fine as a condition of unlocking the computer—and "conservatively" estimating that over $5 million per year is being extorted from ransomware victims).

137. *Cybercrime*, INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (last visited Apr. 1, 2013) ("Cybercrime is one of the fastest growing areas of crime."). Some of our most personal information is now available on the thriving black market for a mere pittance. *How Much Do You Cost on the Black Market?*, OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., http://www.ncix.gov/issues/cyber/identity_theft.php (last visited Apr. 1, 2013) ("[On the black market,] [y]our social security number, at $3, is less expensive than a McDonald's Happy Meal.").

when you factor in downtime),[138] and a highly controversial McAfee estimate places cybercrime losses as high as $1 trillion in 2010 alone.[139]

2. Professionalization and Commoditization of Cybercrime

Cybercriminals have grown increasingly sophisticated, both in terms of business models[140] and in terms of tools,[141] leading cybercrime experts to warn that we have entered an era of cybercrime "professionalization" and

138. Press Release, Symantec, Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually (Sept. 7, 2011), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (describing the methodology for arriving at the $114 billion and $388 billion figures as "extrapolations" based on a survey of over 12,000 adults conducted in twenty-four countries).

139. *See* Robert Richardson, *Bigger Than a Trillium*, COMPUTER SEC. INST., http://gocsi.com/public/trillium (last visited Apr. 1, 2013) (explaining that the $1 trillion estimate comes not from a McAfee report, but from company talking points); *Keith Alexander's Remarks*, *supra* note 74, at 09:29 ("McAfee estimates that $1 trillion was spent globally on remediation."); *see also* President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/video/President-Obama-on-Cybersecurity#transcript (citing McAfee's estimate of $1 trillion in cybercrime losses). *But see* Andy Greenberg, *McAfee Explains the Dubious Math Behind Its 'Unscientific' $1 Trillion Data Loss Claim*, FORBES (Aug. 3, 2012), http://www.forbes.com/sites/andygreenberg/2012/08/03/mcafee-explains-the-dubious-math-behind-its-unscientific-1-trillion-data-loss-claim/ (questioning the validity of the $1 trillion estimate, which McAfee has called a "ballpark figure" and "unscientific," but noting that McAfee stands by the estimate, saying that it was not simply made up); Peter Maas & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012, 11:12 AM), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion (criticizing the validity of the $1 trillion estimate and reporting that Ross Anderson, a well-known security researcher at the University of Cambridge, called the "intellectual quality" of the $1 trillion estimate "below abysmal"). *See generally* ROSS ANDERSON ET AL., MEASURING THE COST OF CYBERCRIME (June 26, 2012), http://lyle.smu.edu/~tylerm/weis12pres.pdf (calling existing cybercrime estimates "eye-poppingly large," identifying methodological flaws in certain reports on costs of cybercrime, and offering a framework for analyzing the costs of cybercrime).

140. *See* TRENDMICRO, THE BUSINESS OF CYBERCRIME: A COMPLEX BUSINESS MODEL 5 (2010), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf ("[C]yber scams are often part of an intricate, highly sophisticated and highly organized [cybercrime] business model based on the concept of affiliate marketing."); Jim Finkle, *Inside a Global Cybercrime Ring*, REUTERS (Mar. 24, 2010, 11:12 AM), http://www.reuters.com/article/2010/03/24/us-technology-scareware-idUSTRE62N29T20100324 (describing Innovative Marketing, a "complex underground corporate empire with [cybercrime] operations stretching from Eastern Europe to Bahrain; from India and Singapore to the United States" with estimated revenue of about $180 million in 2008, as a "scareware" pioneer whose programs "pretend to scan a computer for viruses and then tell the user that their machine is infected" in order to scam users into paying to clean their PCs).

141. *See, e.g.*, Rachael King, *Operation High Roller Targets Corporate Bank Accounts*, WALL ST. J. CIO J. (June 26, 2012, 9:07 PM), http://blogs.wsj.com/cio/2012/06/26/operation-high-roller-targets-corporate-bank-accounts/ ("Operation High Roller is characterized by extensive automation.").

"commoditization of attack codes."[142]

With respect to the "professionalization" of cybercrime, there is substantial evidence that cybercriminals are adopting "time-tested business processes to enhance the profitability of crime syndicates worldwide."[143] As one journalist explains:

> The disturbing trend in cybercrime is the "enterprise-class" approach crime syndicates take to grow their businesses. Today's syndicates employ hierarchies of participants with roles that mirror the executive suite, middle management and the rank and file. The executive suite oversees strategy and operations that initiate nefarious acts. Recruiters identify "infantry" that carry out large-scale attack schemes on a permanent hire or outsource (affiliate) basis. They also . . . mold reward programs to pay affiliates once successful attacks are carried out . . . . [W]ith creative profit-sharing flair, crime syndicates are continuing to grow sophisticated pay-per-click/install/purchase affiliate programs to reward up and coming cybercriminal affiliates on a performance-based scale. [And] taking a page out of Wall Street, crime syndicates are engaging in mergers and acquisitions to grow their botnets . . . .[144]

Simultaneously, we are witnessing the commoditization of cybercrime tools. While hacking once required considerable technical expertise, cybercrime toolkits are now available as commodities on the black market,[145] as are so-called "zero-day" exploits, which are used to exploit

---

142. Tom Kellermann, Panel 1: The Promise and Peril of Being Interconnected, Interoperable, and Intelligent at the American University Law Review Symposium: America the Virtual: Security, Privacy, and Interoperability in an Interconnected World (Oct. 25, 2012), *available at* http://www.aulawreview.com/index.php?view=vidlink&catid=1:symposium-2012&id=155:promise-and-peril-of-interconnectivity&option=com_vidlinks&Itemid=150 ("You no longer need to learn to build a gun to learn to pull the trigger . . . [adversaries] don't have to build an AK-47; they just need to learn to use it.").

143. Derek Manky, *Why Cybercrime Remains Big Business – And How to Stop It*, FORBES (Feb. 1, 2013, 5:07 PM), http://www.forbes.com/sites/ciocentral/2013/02/01/why-cybercrime-remains-big-business-and-how-to-stop-it/.

144. *Id.* (describing how competition between two rival crimeware kits—Zeus and SpyEye—hurt profits for both, leading the botnet owners to "merge[] source code, retire[] Zeus support, and pass[] the torch to SpyEye.").

145. *See id.* ("Zeus, circa 2007, peaked in 2010 as the most prolific banking crime kit around. The crimeware kit would create new versions of powerful malware which had the capability to steal banking credentials, as well as hijack and manipulate secure online banking sessions."); RSA, RSA 2012 CYBERCRIME TRENDS REPORT: THE CURRENT STATE OF CYBERCRIME AND WHAT TO EXPECT IN 2012 (2012), http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf ("The more savvy criminals offer their goods and services to those who may be starting out or are in need of set-up and instructions. Whether selling off-the-shelf botnets, Trojans by the binary, or Zeus recompiles, the underground is loaded with tools to allow any 'newbie' cybercriminal to launch an attack.").

previously unknown vulnerabilities.[146] The black market demand for such exploits is driven by those who lack the "technical sophistication to find their own vulnerabilities and launch attacks," and the black market functions relatively efficiently with "Google-like search engines connect[ing] those who have discovered the vulnerability with customers who have the money to buy the knowledge," whether nation-states, criminals, terrorists, or hacktivists.[147]

B. Cyberespionage

> *Every major company in the United States has already been penetrated by China.*
> *-Richard Clarke, former White House counterterrorism expert and special advisor on cybersecurity to President Clinton*[148]

"Cyberespionage" in this Article refers to state-sponsored theft of industrial and defense secrets and/or intellectual property.[149] General Keith Alexander, who is dual-hatted as director of the NSA and chair of U.S. Cyber Command,[150] recently characterized the volume of intellectual

---

146. Andy Greenberg, *Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:40 AM), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (documenting the black market for so-called "zero-day" exploits or "cyberweaponry"); Stew Magnuson, *Growing Black Market for Cyber-Attack Tools Scares Senior DoD Official*, NAT'L DEF. MAGAZINE (Feb. 22, 2013, 2:49 PM), http://www.nationaldefensemagazine.org/blog /Lists/Posts/Post.aspx?ID=1064 ("There has been a black market for those willing to sell knowledge of [zero-day exploits] for years. That market has now moved into the world of supervisory control and data acquisition (SCADA) systems that run power plants," according to Eric Rosenbach, deputy assistant secretary of defense for cyber policy).

147. Magnuson, *supra* note 146 ("[The] growing black market for zero-day vulnerabilities is allowing almost anyone with the cash to buy the means to launch destructive cyber-attacks against U.S. industrial control systems . . . .").

148. Ron Rosenbaum, *Richard Clarke on Who Was Behind the Stuxnet Attack*, SMITHSONIAN MAG. (Apr. 2012), http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html?c=y&story=fullstory.

149. *See* Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyberwar?*, THE NEW YORKER (Nov. 1, 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

150. Cyber Command, or CYBERCOM, "coordinates defense of the military part of the Internet, the '.mil' domain, and conducts offensive computer network operations as ordered." SPADE, *supra* note 23, at 28. *See U.S. Cyber Command Factsheet*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command/ (last updated Dec. 2011) ("USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while

property theft the United States experiences as "astounding"[151] and publicly stated that, in his opinion, it is the "greatest transfer of wealth in history."[152]

Some prominent examples of cyberespionage include: Moonlight Maze (1998);[153] Byzantine Hades (2002);[154] Operation Titan Rain (2003);[155]

---

denying the same to our adversaries."); *see also* Joanna Stern & Luis Martinez, *Pentagon Cyber Command: Higher Status Recommended*, ABC NEWS (May 2, 2012), http://abcnews.go.com/Technology/pentagon-cyber-command-unit-recommended-elevated-combatant-status/story?id=16262052#.UMU444QgqY.

151. *Keith Alexander's Remarks*, *supra* note 74, at 34:30.

152. *Id.* at 09:06-09:11. Cybersecurity expert Dmitri Alperovitch, the Chief Technology Officer of CrowdStrike, Inc., appears to have coined this phrase in August 2011 while working as Vice President of Threat Research at McAfee, Inc. *See* ALPEROVITCH, *supra* note 96, at 2 ("What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition (SCADA) configurations, design schematics, and much more has 'fallen off the truck' of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries."); *see also* Dean Takahashi, *Black Hat's Spotlight Falls on McAfee's Dmitri Alperovitch for Uncovering Cyberspying*, VENTURE BEAT (Aug. 4, 2011, 7:00 AM), http://venturebeat.com/2011/08/04/black-hats-spotlight-falls-on-mcafees-dmitri-alperovitch-for-uncovering-cyber-spying/ (quoting Alperovitch, who called the widespread, China-based "Shady RAT" cyberespionage campaign the "biggest transfer of wealth in terms of intellectual property in human history").

153. Moonlight Maze refers to a series of intrusions into the U.S. Department of Defense ("DoD") computers that began in March 1998 and lasted for three years. Moonlight Maze probed computers at NASA, the Pentagon, the Department of Energy, and private institutions, accessing "troop configurations, maps of military installations, and military hardware designs" in what was then deemed the "largest sustained cyber-attack on the United States." Jessica Bourquin, The Evolution of Cyber Espionage: A Case for an Offensive U.S. Counterintelligence Strategy 11 (Oct. 14, 2011) (unpublished student white paper), *available at* https://www.treadstone71.com/index.php/news-info-whitepapers/masters-in-cybersecurity-intelligence-and-forensics/doc_download/48-the-evolution-of-cyber-espionage-jessica-bourquin. Experts traced the attacks to Moscow but could not confirm that Russia was responsible for the attacks. *Id.* at 12.

154. Byzantine Hades refers to a decade-long series of attacks believed to be perpetrated by the Chinese military. Brian Grow & Mark Hosenball, *Special Report: In Cyberspy vs. Cyberspy, China Has the Edge*, REUTERS (Apr. 14, 2011, 3:52 PM) http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414 ("Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches – colorfully named "Byzantine Hades" by U.S. investigators – to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.") These attacks, which generally rely on spear-phishing, have resulted in the exfiltration of terabytes of sensitive information from the U.S. government and private sector companies, including "designs for multi-billion dollar weapons systems," see id., such as the blueprints for the "quiet electric drive" that U.S. submarines use for stealth operation. Bourquin, *supra* note 153, at 13; Mathew J. Schwartz, *Leaked Cables Indicate Chinese Military Hackers Attacked U.S.*,

Operation Buckshot Yankee (2008);[156] Operation Night Dragon (2008–2011);[157] Operation Aurora (2009);[158] penetration of Lockheed Martin,

---

INFORMATIONWEEK (Apr. 19, 2011, 1:09 PM), http://www.informationweek.com/security/attacks/leaked-cables-indicate-chinese-military/229401866; Michael Riley and John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, BLOOMBERG (Dec. 14, 2011, 8:47 AM), http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html.

155. "Operation Titan Rain" refers to a series of security breaches that targeted sensitive, but unclassified information. The Department of Defense "has acknowledged that the majority of such incidents . . . were orchestrated by China as a method of cyber-espionage." Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 829 (2012). Beginning in 2003, the Titan Rain cyberespionage team successfully exfiltrated sensitive information from DoD as well as private sector companies supporting the military's mission. Exfiltrated data included copies of U.S. Air Force flight-planning software, "specifications for the aviation-mission-planning system used in Army helicopters," and "hundreds of detailed schematics on propulsion systems." Bourquin, *supra* note 153, at 15.

156. In 2008, DoD "suffered a significant compromise of its classified military computer networks." Melissa E. Hathaway, *Leadership and Responsibility for Cybersecurity*, GEO. J. OF INT'L AFF. (2012), at 71, 72. Specifically, Central Command, which was overseeing the wars in Iraq and Afghanistan, was penetrated through an infected USB drive. "Operation Buckshot Yankee" was the codename for recovery from this incident. *Id.*

157. "Night Dragon" is the code name for a cyberespionage campaign leveled against six global oil, energy, and petrochemical companies, including Exxon Mobil, Royal Dutch Shell, and BP. The attack has been described as a "systemic long-term compromise of [the] Western oil and gas industry." ALPEROVITCH, *supra* note 96, at 2. It is believed to have lasted from 2008 to 2011, during which time Chinese cyberspies are alleged to have stolen valuable intellectual property including: bidding information, prospecting data including computerized topographical maps worth "millions of dollars" that show locations of potential oil reserves, and highly sensitive confidential business information. Michael Riley, *Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers*, BLOOMBERG (Feb. 24, 2011, 3:26 AM), http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html. The tools, techniques, and network activities associated with the attack were traced back to China. ALPEROVITCH, *supra* note 96, at 2.

158. "Operation Aurora" refers to a successful Chinese cyberespionage campaign against Google and thirty-three other major U.S. companies (reportedly including Intel, Dow Chemical, Morgan Stanley, and computer security guru, Symantec). While reports initially suggested that the cyberspies were trying to hack primarily into Gmail accounts of Chinese dissidents as part of an effort to quell dissent, security experts later opined that the cyberspies were in fact targeting Google's sensitive systems and intellectual property. David Drummond, *A New Approach to China*, GOOGLE PUB. POL'Y BLOG (Jan. 12, 2010, 6:53 PM), http://googlepublicpolicy.blogspot.com/2010/01/new-approach-to-china.html. Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES, (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html (reporting that leaked American diplomatic cables indicate that "China's Politburo directed the intrusion into Google's computer systems," and that the "Google hacking was part of a coordinated campaign of computer sabotage carried out [in part] by government operatives").

BAE Systems and Northrop Grumman (2009);[159] Operation Shady RAT (2006);[160] GhostNet (2009);[161] the RSA Breach (2011);[162] and twenty-three natural gas pipeline operators (December 2011–June 2012).[163]

---

159. Chinese cyberspies are alleged to have stolen several terabytes of classified data related to the design and electronics system of the F-35 Joint Strike Fighter, the Pentagon's $300 billion weapons project. Specifically, in 2009, cyberspies attacked networks belonging to several major western defense contractors, including Lockheed Martin and Northrop Grumman in the United States and BAE Systems in the United Kingdom. *See* Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J. (Apr. 21, 2009), http://online.wsj.com/article/SB124027491029837401.html.

160. "Operation Shady RAT" refers to a five-year cyberspying campaign allegedly perpetrated by the Chinese that successfully penetrated the computer networks of more than seventy governments and major corporations (including thirteen defense contractors) in fourteen countries. Approximately fifty targets were in the United States. The list of governments and institutions believed to have been infiltrated includes the United States, Taiwan, Vietnam, Canada, the United Nations, the Olympic committees in three countries, and the International Olympic Committee. *See* ALPEROVITCH, *supra* note 96, at 2–4; Takahashi, *supra* note 152.

161. GhostNet refers to a "vast" malware-based cyberespionage network exposed in 2009 that penetrated more than 1200 computer systems in 103 countries. RON DIEBERT & RAFAL ROHOJINSKI, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK, INFORMATION WARFARE MONITOR 5 (Mar. 29, 2009), http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network; *see* John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES (Mar. 28, 2009), http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all&gwh=0F9A5B2A394E6EF2A8B207B0D8305565. The GhostNet remote access tool may have been created by the same organization as Byzantine Hades. Bourquin, *supra* note 153, at 13.

162. RSA Security's products protect computer networks at the White House, CIA, NSA, Pentagon, Department of Homeland Security ("DHS"), most top defense contractors, and the majority of Fortune 500 companies. RSA is best known for the SecurID key fob that forty million employees across the globe use to remotely access their employer's computer networks. In May 2011, hackers breached the servers at RSA and stole information that could be used to compromise the security of the fobs used to access sensitive corporate and government networks. Chinese hackers are believed to have targeted RSA in order to compromise defense contractors and government agencies using RSA's technology, a view borne out by the fact that shortly after the attack on RSA, Lockheed Martin was attacked using information gained from the RSA attack. *See* Siobhan Gorman & Shara Tibken, *Security 'Tokens' Take Hit*, WALL ST. J. (June 7, 2011), http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html ("[RSA Security] openly acknowledged for the first time that intruders had breached its security systems at defense contractor Lockheed Martin Corp. using data stolen from RSA."). The subsequent investigation revealed that hackers used spearphishing (described at *supra* note 84) to gain access to RSA's servers.

163. Clayton, *supra* note 118 ("Cyberspies linked to China's military targeted nearly two dozen U.S. natural gas pipeline operators over a recent six-month period, stealing information that could be used to sabotage U.S. gas pipelines.").

1. Costs of Cyberespionage

By some reports, cyberespionage is estimated to cost the United States (in terms of lost jobs, innovation, and national security) and its corporations (in terms of lost intellectual property, remediation, and reduced consumer confidence) up to $200 billion annually,[164] but reliably quantifying the potentially staggering costs of cyberespionage has been an elusive goal. Obstacles include the fact that many companies do not know that they have been victimized and even those that do know are often reluctant to disclose out of concern for their reputation. Moreover, "victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits."[165]

2. Advanced Persistent Threats

One particularly insidious form of cyberespionage is known as an advanced persistent threat ("APT"). APTs are highly targeted malware-based attacks[166] with several distinguishing features. First, as their name suggests, APTs are often—though not always—advanced.[167] In many cases, they "utilize the full spectrum of computer intrusion technologies and techniques" and "combine multiple attack methodologies and tools in order to reach and compromise their target."[168] Second, APTs are

164. J. P. London, *Made In China*, 137 U.S. NAVAL INST. PROCEEDINGS MAG. (Apr. 2011), http://www.usni.org/magazines/proceedings/2011-04/made-china#footnotes ("Cyber espionage alone is estimated to cost the United States up to $200 billion a year."); *see* Mike McConnell et al., *China's Cyber Thievery is National Policy—And Must Be Challenged*, WALL ST. J. (Jan. 27, 2012), http://www.boozallen.com/media/file/WSJ-China-OpEd.pdf ("[I]t is also difficult to estimate the economic costs of [cyberespionage] . . . to the U.S. . . . [but] we think it is safe to say that [it is] . . . billions of dollars and millions of jobs.").

165. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE i (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [hereinafter NCIX, FOREIGN SPIES].

166. *See What is Malware?*, MICROSOFT SAFETY & SEC. CTR., http://www.microsoft.com/security/resources/malware-whatis.aspx (last visited Apr. 1, 2013) ("Malware is any kind of unwanted software that is installed without your adequate consent.").

167. *Contra* Kelly Jackson Higgins, *Government Agencies Get Creative in APT Battle*, DARK READING (Oct. 3, 2012, 7:31 PM), http://www.darkreading.com/threat-intelligence/167901121/security/news/240008438/government-agencies-get-creative-in-apt-battle.html (quoting Australian cybersecurity expert David Cottingham, who asserts that APTs are "not actually that advanced at all" and are more like "targeted, persistent threats").

168. *Advanced Persistent Threats (APT)*, DAMBALLA, https://www.damballa.com/knowledge/advanced-persistent-threats.php (last visited Apr. 1, 2013).

persistent.[169] APT operators seek long-term access to their targets, with attack objectives generally extending beyond immediate financial gain.[170] In order to maintain long-term access to targets, APTs generally operate stealthily for as long as possible.[171] Finally, APTs rely on "skilled, motivated, organized and well-funded" operators to coordinate and execute attacks.[172] The substantial resources required to operate APTs generally makes them a tool of nation-states. At their essence, APTs are "computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the 'art of manipulation,' in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information."[173]

APTs traditionally targeted government and military networks.[174] Now, they also target "the defense industrial base and high tech companies, the energy and finance sectors, telecommunications companies as well as media outlets, civil society organizations and academic institutions."[175] Law firms and other small- and medium-sized businesses that work with large companies increasingly are being targeted because they often are entrusted with clients' most sensitive information, yet have weaker cyber defenses.[176]

---

169. Press Release, Mandiant, Mandiant Releases Annual Threat Report on Advanced Targeted Attacks, Mar. 13, 2013, *available at* https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks1/ ("Attackers spend an estimated 243 days on a victim's network before they are discovered.").

170. DAMBALLA, *supra* note 168.

171. *See* Higgins, *supra* note 167 ("Cyberespionage attacks are often camouflaged to maintain their foothold in the victim's network."); DAMBALLA, *supra* note 168 ("[O]perators of APT technologies tend to focus on 'low and slow' attacks—stealthily moving from one compromised host to the next, without generating regular or predictable network traffic—to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.").

172. DAMBALLA, *supra* note 168.

173. *Developments in China's Cyber and Nuclear Capabilities: Hearing Before the U.S.-China Econ. and Security Rev. Comm'n*, 112th Cong. 29 (2012) [hereinafter *Devs. in China's Cyber and Nuclear Capabilities*] (statement of Nart Villeneuve, Senior Threat Researcher, TrendMicro), http://origin.www.uscc.gov/sites/default/files/transcripts/3.26.12HearingTranscript.pdf.

174. *Id.* at 31.

175. *Id.* at 29.

176. *Think That Cyber Espionage Only Happens to Big Companies? Think Again. Hackers Are Targeting Smaller Companies*, RDINSIGHTS (Nov. 5, 2012), http://www.rdinsights.com/2012/11/think-that-cyber-espionage-only-happens-to-big-companies-think-again-hackers-are-targeting-smaller-companies-vendors-and-suppliers/ (asserting that small- and medium-sized businesses have weaker cybersecurity measures "in terms of infrastructure and personnel training" and noting

APTs are likely to remain one of the most serious concerns for U.S. businesses for some years to come,[177] but with the explosive growth of mobile broadband and cloud computing, experts are warning that mobile-malware,[178] including mobile "drive-by-downloads,"[179] and cloud-based attacks[180] may be the "next big thing."

3. Cyberespionage Implications

Regardless of the type of attack and specific attack vector,[181] cyberespionage poses a serious threat to U.S. economic and national security. On the national security side, cyberespionage has been dubbed "the biggest intelligence disaster since the loss of nuclear secrets [in the late 1940s]."[182] Perpetrators "not only gather[] information, but can map networks for future attacks and can leave behind backdoors or malware

---

that without "on-going security auditing" smaller companies may not know if they were hacked or how much client information has been compromised).

177. *Kaspersky Lab Predicts Core Threats for 2013*, NET SEC. (Dec. 6, 2012), http://www.net-security.org/secworld.php?id=14072 ("Kaspersky Lab expects . . . targeted attacks, with the purpose of cyber-espionage, to continue in 2013 and beyond, becoming the most significant threat for businesses.").

178. ESET, TRENDS FOR 2013: ASTOUNDING GROWTH OF MOBILE MALWARE 2 (2012), http://go.eset.com/us/resources/white-papers/Trends_for_2013_preview.pdf ("[W]e see as the main trend for 2013 an exponential growth of mobile malware."); TRENDMICRO, SECURITY THREATS TO BUSINESS, THE DIGITAL LIFESTYLE, AND THE CLOUD: TREND MICRO PREDICTIONS FOR 2013 AND BEYOND 1 (2012), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp-trend-micro-predictions-for-2013-and-beyond.pdf ("The volume of malicious and high-risk Android apps will hit 1 million in 2013.").

179. *See* VERIZON, *supra* note 91, at 27 (explaining that drive-by downloads are auto-executed web-based malware); *Drive-By Downloads: How They Attack and How to Defend Yourself*, TECHNEWSDAILY (May 18, 2012, 9:01 AM), http://www.technewsdaily.com/7789-driveby-download-definition.html ("Drive-by downloads are malicious pieces of software that are downloaded to a computer, tablet or smartphone when the user views a compromised Web page or HTML-based email message. In many cases, the malware will be automatically installed on the system.").

180. NET SEC., *supra* note 177 ("[2013 will bring an] increase in cybercriminal attacks targeting cloud-based services.").

181. An attack vector is the technical term used by cybersecurity experts to describe "the approach used to assault a computer system or network." *Attack Vector*, PC MAG., http://www.pcmag.com/encyclopedia_term/0%2C1237%2Ct%3Dattack+vector&i%3D57711%2C00.asp (last visited Apr. 1, 2013).

182. *War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?*, ECONOMIST (July 1, 2010), http://www.economist.com/node/16478792 (quoting James Lewis at CSIS); *see* Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, U.S. Senators (June 6, 2012), *available at* http://www.hsgac.senate.gov/download/cybersecurity-support-letter-from-top-national-security-leaders ("[The cyberthreat] represents one of the most serious challenges to our national security since the onset of the nuclear age sixty years ago.").

designed to execute or facilitate [a future] attack."[183] With respect to the implications of cyberespionage for economic security, Richard Clarke, the former counterterrorism czar in three U.S. presidential administrations, recently offered this grim warning:

> Every major company in the United States has already been penetrated by China.
>
> . . . .
>
> My greatest fear . . . is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese. And we never really see the single event that makes us do something about it. That it's always just below our pain threshold. That company after company in the United States spends millions, hundreds of millions, in some cases billions of dollars on R&D and that information goes free to China . . . . After a while you can't compete.[184]

4. Perpetrators of Cyberespionage

Many countries—including Russia, France, Israel, India, Japan, and Taiwan—are believed to engage in cyberespionage,[185] but according to most cybersecurity experts, China is in a class by itself.[186] China has both the ability and the motivation to engage in a campaign of cyberespionage,[187] given the close relationship between China's military

183. SPADE, *supra* note 23, at 7.

184. Rosenbaum, *supra* note 148; *see* ALPEROVITCH, *supra* note 96, at 3 ("[I]f even a fraction of [the petabytes of exfiltrated data] is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat not just to individual companies and industries but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world. And let's not forget the national security impact of the loss of sensitive intelligence or defense information.").

185. Hersh, *supra* note 149 ("[According to a] retired four-star Navy admiral . . . Russia, France, Israel, and Taiwan conduct the most cyber espionage against the U.S."); *see also* U.S. DEP'T OF DEF., *supra* note 23, at 6–7 ("Espionage has a long history and is nearly always practiced in both directions. For the U.S. and many other states, traditional espionage has been a state-sponsored intelligence-gathering function focused on national security, defense, and foreign policy issues. The United States Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures. The conduct of all U.S. intelligence operations is governed by long-standing and well-established considerations, to include the possibility those operations could be interpreted as a hostile act.").

186. U.S.-CHINA ECON. & SEC. REV. COMM'N, 2012 REPORT TO CONGRESS 155 (2012), http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf.

187. *See* Stuart Fox, *Hacker Attacks on US Reveal China's Weakness*,

and its state-owned companies;[188] the lack of independent research and development in China;[189] and the state of the Chinese economy.[190] Chinese actors are considered "the world's most active and persistent perpetrators of economic espionage," according to a 2011 National Counterintelligence Executive Report to Congress,[191] and cyberespionage is believed to be an important component of China's long-term economic development strategy.[192] According to three former high-ranking U.S. government officials—the former Director of National Intelligence, Secretary of Homeland Security, and Deputy Secretary of Defense—"[t]he Chinese government has a national policy of economic espionage in cyberspace."[193]

TECHNEWSDAILY (Jan. 11, 2012, 4:32 PM), http://www.technewsdaily.com/7457-chinese-hacking-espionage-weakness.html.

188. *See* U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 186, at 156 ("The state controls up to 50 percent of the Chinese economy, and industrial espionage appears to be a key mission of the Chinese intelligence services."); *see also* REP. MIKE ROGERS & REP. DUTCH RUPPERSBERGER, H. PERMANENT SELECT COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REP. ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE iv (Comm. Print 2011), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (warning U.S. companies and government agencies not to do business with China's Huawei and ZTE, the world's second and fifth largest manufacturers of routers, based on concerns about supply chain security).

189. *See, e.g.*, Michael A. Riley & Ashlee Vance, *China Corporate Espionage Boom Knocks Wind out of U.S. Companies*, BLOOMBERG (Mar. 15, 2012), http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html (paraphrasing Harvard Business School professor Willy Shih's comments that the Chinese "need to build a research and development culture that can supersede their skills at mimicry"); *China's Pharmaceutical Industry Lacks Innovation, Lags Behind*, WORLDWATCH INST., http://www.worldwatch.org/node/3923 (last visited Feb. 18, 2013) ("China's pharmaceutical industry still lacks independent and efficient research and development capabilities . . . ."). *See generally* McConnell et al., *supra* note 164.

190. McConnell et al., *supra* note 164 ("China has a massive, inexpensive work force ravenous for economic growth.").

191. NCIX, FOREIGN SPIES, *supra* note 165, at i; *see* McConnell et al., *supra* note 164 ("Evidence indicates that China intends to help build its economy by intellectual-property theft rather than by innovation and investment in research and development . . . .").

192. Siobhan Gorman, *China Singled Out for Cyberspying*, WALL ST. J. (Nov. 4, 2011), http://online.wsj.com/article/SB10001424052970203716204577015540198801540.html (according to a senior intelligence official, "economic espionage is condoned by both China and Russia and is part of each country's national economic development policy"); KREKEL ET AL., *supra* note 23, at 107 ("The apparent expansion of China's computer network exploitation (CNE) activities to support espionage has opened rich veins of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development.").

193. McConnell et al., *supra* note 164; *see* NCIX, FOREIGN SPIES, *supra* note 165, at 5 (accusing not only China, but also Russia of using cyberespionage to steal U.S.

Although China repeatedly has denied involvement in cyberespionage,[194] there is extensive evidence tying China to cyberespionage campaigns.[195] First, and most obviously, U.S. companies have reported numerous Chinese attempts to steal "client lists, merger and acquisition data, pricing information, and the results of research and development efforts."[196]

Second, the 2013 National Intelligence Estimate ("NIE"), a classified document reflecting the "consensus view of the U.S. intelligence community,"[197] reportedly concluded that "the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness."[198] According to press reports based on interviews of individuals familiar with the report, the NIE identified China "as the country most aggressively seeking to penetrate the computer systems of American business and institutions."[199]

---

industrial secrets as a matter of national policy).

194. In January 2013, the Chinese Defense Ministry stated: "It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence," and in February 2013, Chinese Ministry of Foreign Affairs spokesman HongLei asserted: "China resolutely opposes hacking actions and has established relevant laws and regulations and taken strict law enforcement measures to defend against online hacking activities." David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; *see* Thom Shanker, *U.S. Report Accuses China and Russia of Internet Spying*, N.Y. TIMES (Nov. 3, 2011), http://www.nytimes.com/2011/11/04/world/us-report-accuses-china-and-russia-of-internet-spying.html ("[Chinese] Foreign Ministry spokesman Hong Lei said, 'The Chinese government opposes hacking in all its manifestations.' ").

195. *See, e.g.*, NCIX, FOREIGN SPIES, *supra* note 165, at 5; KREKEL ET AL., *supra* note 23, at 100; Michael Riley & Dune Lawrence, *Hackers Linked to China's Army Seen From EU to D.C.*, BLOOMBERG (July 26, 2012, 7:00 PM), http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html; *see also*, *supra* notes 157–162.

196. Mike Brownfield, *Morning Bell: Stopping the Cyber Espionage Threat*, THE FOUNDRY (Apr. 26, 2012, 9:06 AM), http://blog.heritage.org/2012/04/26/morning-bell-stopping-the-cyber-espionage-threat/.

197. Ellen Nakashima, *U.S. Said To Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets ("Some officials have pressed for an unclassified version of the report to be released publicly, [but] . . . as a matter of policy, [the Office of the Director of National Intelligence does] not discuss or acknowledge the existence of NIEs unless directed to do so.").

198. *Id.*

199. *Id.*; *see* David Barboza, *In Wake of Cyberattacks, China Seeks New Rules*, N.Y. TIMES (Mar. 10, 2013), http://www.nytimes.com/2013/03/11/world/asia/china-calls-for-global-hacking-rules.html ("American intelligence officials have [] said privately that they have evidence of Chinese government involvement in the [recent hacking] attacks.").

Third, just days after the NIE was circulated, U.S. information security company Mandiant released a report of over sixty pages offering extensive evidence of Chinese espionage,[200] including actual video of intrusion activities in action.[201] Based on this evidence, Mandiant said that it believes that since at least 2006, Unit 61398 of China's People's Liberation Army[202] has been conducting an extensive cyberespionage campaign that has resulted in the exfiltration of hundreds of terabytes of data—including "broad categories of intellectual property [such as] technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and e-mails and contacts lists from victim organizations' leadership"—from over 140 companies in twenty major industries.[203] Although not without its critics both in the United States[204] and beyond its borders,[205] the February 13, 2013 Mandiant Report is notable for its public proffer of detailed evidence that China is engaged in extensive government-sponsored cyberespionage campaigns.

---

200. It should be noted that the group behind these attacks is "the same group that [Dmitri] Alperovitch [then Vice President of Threat Research for MacAfee] identified [in 2011]" as having perpetrated Operation Shady RAT. Jody Westby, *Mandiant Report on Chinese Hackers Is Not News But Its Approach Is*, FORBES (Feb. 20, 2013, 8:07 AM), http://www.forbes.com/sites/jodywestby/2013/02/20/mandiant-report-on-chinese-hackers-is-not-news-but-its-approach-is/. In 2011, Dmitri Alperovitch, then vice president of Threat Research for McAfee, authored a report about Shady RAT, the malware that had been used by Chinese cybercriminals to exfiltrate data from a broad cross-section of organizations over a two- to five-year period—undetected. Alperovitch broke new ground when he included a table of more than seventy companies, organizations, and government agencies from around the globe that had been compromised. *Id.*

201. MandiantCorp, *APT1: Exposing One of China's Cyber Espionage Units*, YOUTUBE (Feb. 18, 2013), http://www.youtube.com/watch?v=6p7FqSav6Ho (showing live APT1 Chinese threat actors, codenamed DOTAs, conducting computer network espionage activities).

202. PLA Unit 61398 is formally known as the Second Bureau of the People's Liberation Army General Staff Department's Third Department. MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 3 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

203. *Id.* at 3.

204. *See* Mathew J. Schwartz, *China Denies U.S. Hacking Allegations: 6 Facts*, INFO. WEEK (Feb. 21, 2013, 11:40 AM), http://www.informationweek.com/security/attacks/china-denies-us-hacking-accusations-6-fa/240149058? (noting that Taia Global CEO Jeffrey Carr, who does not dispute that China engages in "massive amounts of cyber-espionage," believes that a more rigorous analysis of Mandiant's APT evidence (e.g., by a "professional intelligence analyst") "would likely have failed to prove attribution").

205. *See, e.g.*, *id.* (discussing Chinese media reports suggesting that the Mandiant report was a "commercial stunt" designed to sell information security products and services); *id.* (citing Chinese government comments describing the Mandiant report as "baseless").

5. Cyberespionage and U.S.-China Relations

Despite the potentially dire economic and national security implications of cyberespionage for the United States, it was only recently, in the face of mounting *public* evidence of the Chinese government's involvement in cyberespionage targeting U.S. companies, that the United States and China began the lengthy, but important, process of diplomatic engagement on the issue.

U.S. media reports of Chinese government-sponsored espionage intensified in the weeks after the Mandiant Report was issued, aggravating existing tensions between the United States and China on cybersecurity and prompting what some have referred to as a "war of words."[206] China's Foreign Minister Yan Jiechi said U.S. reports of Chinese government involvement in cyberespionage were "built on shaky ground" and that "[a]nyone who tried to fabricate or piece together a sensational story to serve a political motive will not be able to blacken the name of others nor whitewash themselves."[207] China increasingly went on the offensive, complaining that it is the victim of hack attacks linked to U.S. Internet Protocol addresses,[208] and the Chinese government repeatedly reasserted its official position that it opposes hacking.

Mounting tensions heightened concerns that U.S. accusations of Chinese cyberespionage would prompt trade-based retaliation from China. Indeed, just a few weeks after the *New York Times* identified Coca-Cola as having been the target of Chinese cyberespionage—in the same article that featured the Mandiant Report[209]—a remote Chinese provincial government announced that it is investigating Coca-Cola for "illegally collecting classified information with handheld GPS equipment."[210] The U.S. company, which is cooperating with the investigation, has denied any wrongdoing and says that it is simply using " 'location-based customer

206. Terril Yue Jones, *U.S., China agree to work together on cyber security*, REUTERS (Apr. 13, 2013, 11:37 AM), http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413.

207. Barboza, *supra* note 199.

208. *Id.* Jones, *supra* note 206 ("China claims it is the victim of large-scale cyber attacks from the United States").

209. Sanger et al., *supra* note 194. A few months earlier, the *New York Times* identified Coca-Cola as the likely unnamed victim of a cyberespionage campaign discussed in a 2010 case study published by Mandiant. Nicole Perlroth, *Study May Offer Insight Into Coca-Cola Breach*, N.Y. TIMES BITS BLOG (Nov. 30, 2012, 4:09 PM), http://bits.blogs.nytimes.com/2012/11/30/study-may-offer-insight-into-coca-cola-breach/.

210. Patti Waldmeir, *Coca-Cola Probed over Mapping in China*, FIN. TIMES (Mar. 12, 2013, 3:43 PM), http://www.ft.com/intl/cms/s/0/f02a6abc-8b21-11e2-b1a4-00144feabdc0.html#axzz2PGMb8mqi.

logistics systems . . .' to improve customer service and fuel efficiency."[211] Regardless of what motivated the Coca-Cola investigation, many U.S. companies are concerned about the potential trade ramifications of confronting China on cyberespionage.

On the other hand, the increasingly public discussion of China's involvement in cyberespionage has not been without benefit. Several noteworthy diplomatic developments came about in the weeks and months following the release of the Mandiant Report. On March 10, 2013, approximately one month after the report was released, China's Foreign Minister took an important diplomatic step, calling for international " 'rules and cooperation' " on Internet espionage issues . . . ."[212] The following day, Tom Donilon, National Security Advisor to the President, delivered a speech to the Asia Society unequivocally setting forth the expectations of the U.S. with respect to China's role in cyberespionage. He said that building a constructive relationship with China is one of the pillars of the U.S. strategy in the Asia-Pacific region, and he identified cybersecurity as a "growing challenge to [the U.S.-China] economic relationship." Donilon said that U.S. cybersecurity concerns have "moved to the forefront of our agenda," and made clear that industrial cyberespionage was an animating concern,[213] stating:

> The international community cannot afford to tolerate such activity from any country. As the President said in the State of the Union, we will take action to protect our economy against cyber-threats. From the President on down, this has become a key point of concern and discussion with China at all levels of our governments. And it will continue to be. The United States will do all it must to protect our national networks, critical infrastructure, and our valuable public and private sector property. But, specifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a

211. *Id.*

212. Barboza, *supra* note 199.

213. "I am not talking about ordinary cybercrime or hacking [and] this is not solely a national security concern or a concern of the U.S. government. Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." Tom Donilon, Nat'l Sec. Advisor to the President, Address to the Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

> constructive direct dialogue to establish acceptable norms of behavior in cyberspace . . . . [T]he United States and China, the world's two largest economies, both dependent on the Internet, must lead the way in addressing this problem.[214]

President Obama himself addressed the issue of nation-state sponsored cyberintrusions just two days later in a March 13 interview, stating: "[w]e've made it very clear to China...that, you know, we expect them to follow international norms and abide by international rules."[215] When newly elected Chinese President Xi Jinping took office on March 14, 2013, President Obama reportedly called to congratulate Xi and took the opportunity to raise U.S. concerns about hacking.[216] In the course of the call, the two leaders reportedly "committed to engage in an ongoing discussion to address the cyber issue."[217]

The conversation between Obama and Xi appears, at least momentarily, to have eased the war of words between China and the United States and to have accelerated formal diplomatic engagement on cybersecurity between the two countries. On March 17, 2013, just days after the Obama-Xi discussion, the new Chinese Premier Li Keqiang said: "I think we should not make groundless accusations against each other, and spend more time doing practical things that will contribute to cyber-security,"[218] and by mid-April 2013, U.S. Secretary of State John Kerry announced that the United States and China had agreed to set up a cybersecurity working group.[219]

While increased diplomatic engagement with China on cybersecurity is encouraging, substantive progress will take time, and, as the U.S. Under Secretary of State for Economic Affairs has noted: "It's important to have a dialogue on this, but it's also important that the dialogue be a means to an end and the end is really ending these practices."[220]

C. Cyberwar

The term "cyberwar" in this Article refers to "actions by a nation-state to penetrate another nation's computers or networks for the purposes of

---

214. *Id.*

215. Steve Holland, *Obama, China's Xi discuss cybersecurity dispute in phone call*, REUTERS (Mar. 14, 2013, 6:03 PM), http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314.

216. *Id.*

217. *Id.*

218. Terril Yue Jones, *China's new premier seeks "new type" of ties with U.S.*, REUTERS (Mar. 17, 2013, 4:02 AM), http://www.reuters.com/article/2013/03/17/us-china-parliament-hacking-idUSBRE92G02320130317.

219. Jones, *supra* note 206.

220. *Id.*

causing damage or disruption."[221] It is believed that "at least 12 of the world's 15 largest militaries are building cyberwarfare programs,"[222] with several nation-states—including the U.S.,[223] China,[224] Russia,[225] Israel,[226]

---

221. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010).

222. Scott Shane, *Cyberwarfare Emerges from Shadows for Public Discussion by U.S. Officials*, N.Y. TIMES (Sept. 26, 2012), http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html. *Cf.* Pierluigi Paganini, *The Rise of Cyberweapons and Relative Impact on Cyberspace*, INFOSEC INST. RESOURCES (OCT. 5, 2012), http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/ (noting that the number of nation-states developing cyberweapons reportedly is as high as 140).

223. Mark Mazzetti & David E. Sanger, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, N.Y. TIMES (Mar. 12, 2013), http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html ("[General Keith Alexander] told Congress [] that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks, the first time the Obama administration admitted to developing such weapons for use in wartime."). The U.S. government "has only recently acknowledged developing cyberweapons, and it has never admitted using them" despite "reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year." David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (discussing what role the United States had in the development of the Stuxnet virus, which successfully destroyed centrifuges at a key Iranian nuclear enrichment facility beginning in 2008); *see* Leon E. Panetta, Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 ("[T]he Department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace."); U.S. DEP'T OF DEF., *supra* note 23, at 5 ("[T]he Department [of Defense] has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests. If directed by the President, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict.").

224. *See generally* KREKEL ET AL., *supra* note 23.

225. *See* Bumiller & Shanker, *supra* note 107; Kim Hart, *Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar*, WASH. POST (Aug. 14, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html?sid=ST2008081303990 (discussing accusations that Russia launched cyberattacks against Georgia's Internet infrastructure, disabling many Georgian government websites and effectively establishing an "information blockade.").

226. *Israel Builds Up Its Cyberwar Corps*, UPI (Nov. 2, 2012, 2:37 PM), http://www.upi.com/Business_News/Security-Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449/ ("Israeli Prime Minister Binyamin Netanyahu established a special division of Unit 8200 [the Israeli equivalent of the NSA] in 2010 to develop [Israel's] cyberwar capabilities."); *see* Sanger, *supra* note 223 (discussing Israel's role in the Stuxnet attack on Iran's nuclear enrichment facilities); *see also* John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES (Sept. 26, 2010),

North Korea,[227] and Iran[228]—already considered to have joined the ranks of the cyberwar-capable. As the "weaponization" of cyber accelerates, mainstream press reports of the cyberwar threat tend to highlight the potentially devastating effects of cyberattacks on our nation's critical infrastructure.[229] These reports describe, *inter alia*, how cyberattacks (1) on the power grid could lead to cascading failures across the nation with catastrophic consequences; (2) on financial systems could lead to economic panic and/or a crashing stock market; (3) on water systems could open dams causing flooding or make entire cities uninhabitable; (4) on rail systems (e.g., involving intentional misrouting of trains) could cause massive collisions; (5) on air-traffic control systems could lead to mass casualties; and (6) on nuclear facilities could result in a nuclear reactor meltdown, leading to catastrophic loss of life.[230] Nonetheless, exactly what constitutes a cyberattack remains ill-defined.

The U.S. military formally distinguishes between two types of offensive cyberpower available to nation-states: Cyber Network Exploitation ("CNE") and Cyber Network Attack ("CNA"). While CNE is essentially espionage, CNA refers to destructive attacks. Specifically, CNAs are

---

http://www.nytimes.com/2010/09/27/technology/27virus.html?hp&_r=0.

227. Tony Capaccio, *North Korea Improves Cyber Warfare Capacity, U.S. Says*, BLOOMBERG (Oct. 23, 2012, 12:45 AM), http://www.bloomberg.com/news/2012-10-23/north-korea-improves-cyber-warfare-capacity-u-s-says.html ("North Korea's government has a 'significant' cyber warfare capability that it continues to improve [according to] the top U.S. commander on the Korean Peninsula.").

228. Ellen Nakashima, *Iran Blamed for Cyberattacks on U.S. Banks and Companies*, WASH. POST (Sept. 21, 2012), http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html ("Iran recently has mounted a series of disruptive computer attacks against major U.S. banks and other companies in apparent retaliation for Western economic sanctions aimed at halting its nuclear program, according to U.S. intelligence and other officials.").

229. The devastating effects of a cyberattack are not necessarily limited to physical effects, but also may include economic and psychological effects (e.g., undermining confidence in systems). *See, e.g.*, SPADE, *supra* note 23, at 26 (noting that a one-day attack on American credit card companies has been estimated to cost $35 billion, and a "full-scale attack" on critical infrastructure could cost $700 billion).

230. *See, e.g.*, Bumiller & Shanker, *supra* note 107 ("An aggressor nation or extremist group could use . . . cyber tools to gain control of critical switches . . . . They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."); Robert Johnson, *New Cyber Attacks Will Target Power Grids and Major Public Works*, BUS. INSIDER (Sept. 14, 2011), http://articles.businessinsider.com/2011-09-14/news/30153012_1_data-theft-turbine-cyber-warfare; Barton Gellman, *Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Web as Tool of Bloodshed, Experts Say*, WASH. POST, June 27, 2002, at A1 ("U.S. analysts believe that by disabling or taking command of the floodgates in a dam, for example, or of substations handling 300,000 volts of electric power, an intruder could use virtual tools to destroy real-world lives and property.").

defined as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[231]

We admittedly have come a long way since 2010 when U.S. Deputy Secretary of Defense William J. Lynn III said, "There's no agreed-on definition of what constitutes a cyberattack."[232] But an important debate continues to rage in military and national security law circles over what, precisely, qualifies as a cyberattack and/or an act of cyberwar[233] and the appropriate range of nation-state responses to such an act.[234] When it comes to an act of cyberwar, "it's in the eye of the beholder."[235]

In November of 2011, the U.S. Department of Defense ("DoD") concluded for the first time that cyberattacks can constitute an act of war[236] to which the United States may respond using traditional military force

---

231. JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 60 (2012), http://www.dtic.mil/doctrine/newpubs/jp102.pdf.

232. Cheryl Pellerin, *Lynn: Cyberspace is the New Domain of Warfare*, U.S. DEP'T OF DEF., AM. FORCES PRESS SERV. (Oct. 18, 2010), http://www.defense.gov/news/newsarticle.aspx?id=61310.

233. *See* Catherine Lotrionte, *Cyber Operations: Conflict Under International Law*, GEO. J. OF INT'L AFF. 15, 16 (2012) ("examin[ing] the challenges in defining the term cyberwar and [] propos[ing] a working definition . . . ."). *See generally* Hathaway et al., *supra* note 155.

234. For example, President Barack Obama's *International Strategy for Cyberspace* released in May 2011 marked the first time that the U.S. expressed the position that it would regard cyberattacks as on par with conventional attacks. *See* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 28, at 14 ("When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."); *id.* ("We reserve the right to use all necessary means—diplomatic, informational, military and economic . . . in order to defend our Nation, our allies, our partners and our interests."). In a veiled reference to Article 5 of the NATO charter requiring allies to regard an attack against any member as an attack against all, the strategy stated: "we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners." *Id.*

235. Ellen Nakashima, *U.S. Cyber Approach 'Too Predictable' for One Top General*, WASH. POST (July 14, 2011), http://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html (quoting a July 2011 comment made by General James Cartwright, former vice chairman of the Joint Chiefs of Staff).

236. U.S. DEP'T OF DEF., *supra* note 23, at 9 ("The phrase 'act of war' is frequently used as shorthand to refer to an act that may permit a state to use force in self-defense, but more appropriately, it refers to an act that may lead to a state of ongoing hostilities or armed conflict. Contemporary international law addresses the concept of 'act of war' in terms of a 'threat or use of force,' as that phrase is used in the United Nations (UN) Charter. Article 2(4) of the UN Charter provides: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.' ").

(i.e., a kinetic, rather than cyber-based, response).[237] According to one military official, the basic concept is "[i]f you shut down our power grid, maybe we will put a missile down one of your smokestacks."[238] In its 2011 report to Congress announcing its decision, DoD stated:

> [T]he President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interest from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government, or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by DoD.[239]

Notwithstanding DoD's report, defense officials continue to struggle to define exactly what kind of cyberattack constitutes a "use of force" (the equivalent of an armed attack), with some officials of the opinion that the test should be whether or not a cyberattack has an effect equivalent to a conventional attack.[240] Others argue that what is important is the amount of "actual or attempted" damage caused by the attack.[241]

Some early examples of "cyberattacks" include: (1) "Web War I,"[242] in which Russia initiated a barrage of distributed denial of service ("DDoS") attacks on Estonia's "essential electronic infrastructure" in 2007 in response to Estonia's then-controversial decision to relocate a Soviet-era memorial to fallen WWII soldiers;[243] and (2) coordinated Russian cyberattacks on Georgia's Internet infrastructure in connection with the brief war between Russia and Georgia in 2008.[244] Cyberattacks also have

---

237. *Id.* at 4; *see* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J. (May 30, 2011, 10:30 PM), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html (discussing Pentagon thinking on the issue of what kinds of cyberattacks would be considered a "use of force" potentially triggering retaliation); *id.* ("One idea gaining momentum at the Pentagon is the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a 'use of force' consideration, which could merit retaliation.").

238. *Id.*

239. U.S. DEP'T OF DEF., *supra* note 23, at 4.

240. Gorman & Barnes, *supra* note 237.

241. *Id.*

242. *War in the Fifth Domain*, *supra* note 182.

243. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all ("All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.").

244. David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J. 1, 2–5 (Jan. 6, 2011), http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

been reported more recently in the ongoing conflicts between North and South Korea,[245] and Israel and Hamas.[246] In contrast, the United States reportedly declined to engage in offensive cyberattacks during the U.S.-led strikes on Libya in March 2011.[247]

High-profile "cyberattacks" emanating from, directed at, or intended to influence the United States reportedly include: (1) Stuxnet; (2) Wiper; (3) Shamoon; and (4) the summer 2012 denial of service attacks on U.S. financial institutions. Each is described in more detail below.

First, the Stuxnet virus reportedly was unleashed as part of a U.S.-Israeli operation to destroy centrifuges at Iran's Natanz nuclear enrichment complex.[248] The operation reportedly began under President George W. Bush and was intended to sabotage Iran's nuclear program.[249] Discovered in June 2010, Stuxnet was "the first attack of a major nature in which a cyberattack was used to effect physical destruction."[250]

Second, like Stuxnet, the Wiper virus reportedly was created by the United States and Israel and was used to systematically delete data and system files from computers as part of an April 2012 cyberattack on Iran's Oil Ministry and affiliates, including the National Iranian Oil Company.[251]

(explaining that Russia used cyber operations to disrupt the Georgian government's ability to communicate strategically with the international community); Robert Haddick, *This Week At War: Lessons From Cyberwar I*, FOREIGN POL'Y (Jan. 28, 2011), http://www.foreignpolicy.com/articles/2011/01/28/this_week_at_war_lessons_from_cyberwar_i ("When the kinetic battle broke out on Aug. 7, Russian government and irregular forces conducted distributed denial-of-service attacks on Georgian government and military sites. These attacks disrupted the transmission of information between military units and between offices in the Georgian government. Russian cyberforces attacked civilian sites near the action of kinetic operations with the goal of creating panic in the civilian population. Russian forces also attacked Georgian hacker forums in order to pre-empt a retaliatory response against Russian targets.").

245. Pierluigi Paganini, *Concerns Mount over North Korean Cyber Warfare Capabilities*, INFOSEC ISLAND (June 11, 2012), http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.

246. Gwen Ackerman & Saud Abu Ramadan, *Israel Wages Cyberwar with Hamas as Civilians Take up Computers*, BLOOMBERG (Nov. 19, 2012, 5:08 PM), http://www.bloomberg.com/news/2012-11-19/israel-wages-cyber-war-with-hamas-as-civilians-take-up-computers.html.

247. Eric Schimtt & Tom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html. American officials "rejected cyberwarfare" out of (1) concern that it might "set a precedent for other nations . . . to carry out such offensives"; (2) concern about mounting the attack "on such short notice"; and (3) inability "to resolve whether the president had the power to proceed with such an attack without informing Congress." *Id.*

248. Sanger, *supra* note 223.

249. *Id.*

250. *Id.*

251. Kim Zetter, *Qatari Gas Company Hit with Virus in Wave of Attacks on Energy*

As one Iranian official explained, "The aim [of Wiper] is to increase pressure so that Iran will compromise in the upcoming nuclear talks on May 23[, 2012]."[252]

Dubbed a "Wiper copycat,"[253] the Shamoon virus was discovered August 16, 2012, after attacking 30,000 computers at Saudi Arabia's state-owned oil company (Aramco) and replacing critical files on those computers with images of a burning American flag. Although the United States has not officially blamed Iran for the attack, it is widely believed that Iran launched the attack in retaliation for Stuxnet. Iran likely targeted Aramco because the company supplied oil to customers who were unable to get oil from Iran after U.S.-led financial sanctions cut Iran's oil exports nearly in half.[254] Just weeks after the Aramco attack, Shamoon attacked computers at Qatar's RasGas, one of the world's largest exporters of liquefied natural gas.[255]

Iran also is believed to be behind the prolonged denial of service attacks against major U.S. financial institutions launched in September 2012, including Bank of America, Wells Fargo, PNC, and others.[256]

If media reports are any indication, concerns over cyberwar appear to have intensified throughout 2012 at the highest levels of the U.S. government, with dire warnings repeatedly emanating from top U.S. defense officials. DHS Secretary Janet Napolitano warned in November 2011 that a cyberattack on critical infrastructure could cause "loss of life" and "huge economic loss."[257] The following summer, six elite U.S.

Companies, WIRED (Aug. 30, 2012, 5:04 PM), http://www.wired.com/threatlevel/2012/08/hack-attack-strikes-rasgas/.

252. Thomas Erdbrink, *Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals from Internet*, N.Y. TIMES (Apr. 23, 2012), http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html.

253. Elinor Mills, *A Who's Who of Mid-East Targeted Malware*, CNET (Aug. 31, 2012, 4:00 AM), http://news.cnet.com/8301-1009_3-57503949-83/a-whos-who-of-mideast-targeted-malware/; Erdbrink, *supra* note 252.

254. Siobhan Gorman & Julian A. Barnes, *Iran Blamed for Cyberattacks: U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy*, WALL ST. J. (Oct. 12, 2012, 7:38 PM), http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html; *see* Nicole Perlroth, *Connecting the Dots After Cyberattack on Saudi Aramco*, N.Y. TIMES BITS BLOG (Aug. 27, 2012, 7:20 PM), http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-after-cyberattack-on-saudi-aramco/.

255. Zetter, *supra* note 251.

256. *See* Nicole Perlroth, *Attacks on 6 Banks Frustrate Customers*, N.Y. TIMES (Sept. 30, 2012), http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html; Chris Strohm & Eric Engleman, *Cyber Attacks on U.S. Banks Expose Vulnerabilities*, BUSINESSWEEK (Sept. 28, 2012), http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability.

257. Jason Ryan, *Loss of Life in Major Computer Attack, Warns Homeland Security*,

national security officials[258] urged Congress to pass cybersecurity legislation to protect critical infrastructure, writing:

> We carry the burden of knowing that 9/11 might have been averted with the intelligence that existed at the time. We do not want to be in the same position again when 'cyber 9/11' hits—it is not a question of 'whether' this will happen; it is a question of 'when.'[259]

In the fall of 2012, then-Defense Secretary Leon Panetta warned that the U.S. is at risk for a "cyber-Pearl Harbor[;] . . . an attack that would cause physical destruction and the loss of life . . . and create a profound new sense of vulnerability."[260] Panetta said:

> A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation . . . . The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks.[261]

Finally, in an op-ed published in the *New York Times* on December 6, 2012 to coincide with the anniversary of Pearl Harbor, Senators Lieberman and Collins warned:

> A storm is surely gathering again, and we must resist the false sense of calm. The attack is not a matter of if, but when. It will not be launched

---

ABC NEWS (Oct. 27, 2011, 6:33 PM), http://www.homelandsecuritynewswire.com/dr20111201-congressional-approval-of-cybersecurity-bill-looks-promising.

258. Namely, Michael Chertoff, former Secretary of the Department of Homeland Security; Mike McConnell, former Director of the NSA and former Director of National Intelligence; Paul Wolfowitz, former Deputy Secretary of Defense; Michael Hayden, retired U.S. Air Force four-star general and former Director of both the NSA and the CIA; James Cartwright, retired U.S. Marine Corps four-star general and former Vice Chairman of the Joint Chiefs of Staff; and William Lynn III, a former Deputy Secretary of Defense. Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, *supra* note 182.

259. *Id.*

260. Bumiller & Shanker, *supra* note 107. Testifying before the Senate Armed Services Committee in June, 2011, then-Secretary of Defense Leon Panetta said, "The next Pearl Harbor we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems." *Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense Before the S. Comm. on Armed Services*, 112th Cong. 25 (June 9, 2011) [hereinafter *Panetta Confirmation Hearing*] (statement of Leon Panetta), http://www.armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf.

261. Panetta, *supra* note 223.

> from aircraft carriers, missile silos or massed armies. It will come through cyberspace and will strike our most vital computer systems, those that manage our electricity grids, oil and gas pipelines, telecommunications networks and financial markets. We know that our digital networks are being tested, on a minute by minute basis, by would-be cyberterrorists, criminal gangs, rogue hackers and rival nations who look for unguarded digital back doors that would allow them to seize control of our most essential computers.[262]

Some experts have suggested that cyberwar concerns have been greatly exaggerated. For example, a recent Dartmouth study of cyberwar funded by DHS concluded that "the degree of damage that could be caused in a cyberattack bears no resemblance to an electronic 'Pearl Harbor,' " although "inflicting significant economic costs on the public and private sectors and impairing performance of key infrastructures (via IT networks linked to embedded computer systems, for example) seem both plausible and realistic."[263] Prominent cybersecurity expert James Lewis at the Center for Strategic and International Studies ("CSIS") has repeatedly expressed skepticism of the view that cyberattacks are likely to cause widespread death, damage, and destruction. In a 2003 interview, he said:

> [N]o sane person argues—that a cyber attack could lead to mass casualties. It's not in any way comparable to weapons of mass destruction. In fact, what a lot of people call them is 'weapons of mass annoyance.'[264] If your power goes out for a couple hours, if somebody draws a mustache on Attorney General Ashcroft's face on his Web site, it's annoying. It's irritating. But it's not a weapon of mass destruction. The same is true for this.[265]

---

262. Joseph I. Lieberman & Susan Collins, *At Dawn We Sleep*, N.Y. TIMES (Dec. 6, 2012), http://www.nytimes.com/2012/12/07/opinion/will-congress-act-to-protect-against-a-catastrophic-cyberattack.html.

263. BILLO & CHANG, *supra* note 23, at 7. "Some experts maintain that cyberattacks with potential strategic national security effects, often referred to as an 'electronic Pearl Harbor,' are impossible. Others proclaim they are inevitable." *Id.* at 12.

264. The phrase "weapons of mass annoyance" was coined by Stewart Baker. JAMES A. LEWIS, CTR. FOR STRATEGIC & INT'L STUDIES, ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR, AND OTHER CYBER THREATS, 11 n.2 (2002), http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

265. *Frontline: Cyberwar!: Interview of James A. Lewis*, (PBS television broadcast Feb. 18, 2003), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html; *see* LEWIS, *supra*, note 264, at 11 ("Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber-terrorism and cyber-warfare give them credit for, and cyber attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring

Writing in a similar spirit in 2010, Lewis explained: "[c]yberattacks are not very destructive, compared to other weapons, particularly strategic weapons. It seems fair to say that at this time, the possibility of damage, death and destruction from cyber attack is low. Cyber weapons will have difficulty produc[ing] casualties."[266]

The broad spectrum of expressed views as to the severity of the cyberthreat may be indicative of both the reality and unpredictability of the threat. As Chairman of the Joint Chiefs of Staff General Martin Dempsey stated in 2012, "Cyber is the black swan[267] because we don't know exactly what capabilities exist out there . . . . If you're asking me which of the unknown threats worry me the most—cyber . . . . Cyber is the threat that concerns me the most."[268]

While acknowledging the gravity of the cyber threat, intelligence officials dramatically toned down their cyberwar rhetoric in early 2013. For example, while Director of National Intelligence ("DNI") James Clapper told Congress in March 2013 that cyberattacks are the most dangerous threat facing the United States, he also said that the intelligence community sees only a "remote chance" of a major computer attack on the United States in the next two years.[269]

Rhetoric aside, experts are struggling to identify appropriate responses to nation-state cyberattacks.[270] The administration took a small step forward with respect to one aspect of these difficult issues in mid-October, when President Obama reportedly signed Presidential Decision Directive 20 ("PDD-20").[271] Although classified, PDD-20 guides federal agency

---

service than early analysts realized. Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cyber crime may be not be fully appreciated by many observers.").

266. LEWIS, *supra* note 264, at 3.

267. *Black Swan Definition*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/black%2Bswan (last visited Apr. 1, 2013) (defining "black swan" as "an unpredictable or unforeseen event, typically one with extreme consequences . . . .").

268. ForaTv, *Martin Dempsey: Cyber Attacks are Black Swan Threat to US*, YOUTUBE (Aug. 22, 2012), http://www.youtube.com/watch?v=aDAG1dJNu4Q.

269. Mazzetti & Sanger, *supra* note 223 (describing a "major" attack as one resulting in "long-term, wide-scale disruption of services, such as a regional power outage").

270. Jonathan Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV., no. 3, 2010, at ¶ 1 ("Cyber attacks do not fit neatly into the traditional international framework governing the use of force.").

271. Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, WASH. POST (Nov. 14, 2012), http://www.washingtonpost.com/world/national-

responses to cyberthreats and "attempts to settle years of debate among government agencies about who is authorized to take what sorts of actions in cyberspace and with what level of permission."[272] PDD-20 reportedly is "the most extensive White House effort to date to wrestle with what constitutes an 'offensive' and a 'defensive' action in the rapidly evolving world of cyberwar and cyberterrorism."[273]

As experts debate the proper definition and response to nation-state cyberattacks,[274] another great challenge looms: understanding how we, as a nation, should address the threat of state actors engaging in highly disruptive (and potentially economically destabilizing) activities in the .com domain—e.g., electronically manipulating the stock market or triggering communications outages—that are not accompanied by the loss of life or physical destruction typically associated with acts of war. While some support giving U.S. Cyber Command the flexibility to defend critical infrastructures against cyberthreats, others have deep concerns about allowing the military to operate outside of the .mil context, including concerns that military cyberoperations could lead to unintentional collateral damage, such as shutting down a hospital generator.

Finally, compounding the cyberwar threat is an increasingly sophisticated, and entirely unregulated, market for so-called "zero-day" exploits.[275] Zero-day exploits are previously unknown cyber-vulnerabilities that can be used in a cyberattack.[276] Some liken zero-day exploits to cyberweapons[277] because they essentially "provide keys to the doors through which cyberwarfare can be waged."[278] Hackers and others who discover such exploits can make their findings public, work with vendors to fix the security flaws, use the exploits for their own purposes, or sell the exploits to security firms, black-marketers, or nation-states. Some hackers have even suggested that corporate IT departments could become profit centers by developing offensive exploits and selling them to the United States and allied governments.[279] Nation-states may purchase

---

security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

272. *Id.* (describing contents of PDD-20).

273. *Id.*

274. *See* Ophardt, *supra* note 270, at ¶ 1.

275. *See generally* Greenberg, *supra* note 146 (documenting the black market for so-called "zero-day" exploits or "cyberweaponry").

276. *Id.*

277. *Id.* (quoting privacy activist Chris Soghoian that "zero-day" exploits are the "bullets for cyberwar").

278. Ophardt, *supra* note 270, at ¶ 18.

279. Jeffrey Carr, *Flipping Malware: A Profit Opportunity for Corporate IT Departments*, INFOSEC ISLAND (Dec. 9, 2012), http://www.infosecisland.com

exploits with the "explicit intention of invading or disrupting the computers and phones of crime suspects and intelligence targets."[280] Accordingly, some hackers reportedly "self-regulate," limiting the foreign interests to whom they are willing to sell or refusing to sell to foreign interests at all.[281]

V. RECENT CONGRESSIONAL AND EXECUTIVE ACTION

One of the most fundamental cybersecurity issues facing our nation is the appropriate role of government in helping the private sector—which owns and operates approximately 85% of the United States' critical infrastructure[282]—address cybersecurity risks to its operations. Although the U.S. has long relied primarily on a market-based approach to cybersecurity, a host of laws and regulations, some of which were passed over a decade ago, have effectively forced cybersecurity investment in certain industry sectors, most notably the financial and health sectors.[283]

/blogview/22777-Flipping-Malware-A-Profit-Opportunity-for-Corporate-IT-Departments.html.

280. Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)*, FORBES (Mar. 21, 2012, 9:08 AM), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/.

281. *Id.* (reporting that vulnerability research company, Vupen, claims that it carefully screens its clients, selling only to NATO governments and "NATO partners," but that Vupen admits that there is no way to ensure that clients will not sell its products to another entity).

282. *See* TELECOMMS. INDUS. ASS'N, SECURING THE NETWORK: CYBERSECURITY RECOMMENDATIONS FOR CRITICAL INFRASTRUCTURE AND THE GLOBAL SUPPLY CHAIN 1 (2012), http://tiaonline.org/sites/default/files/pages/TIACybersecurityWhitePaper_0.pdf (estimating that approximately eighty to ninety percent of the nation's critical infrastructure is privately-owned); *see also* SPADE, *supra* note 23, at 25 ("[Privately-owned telecommunications companies] own and operate most of America's cyber infrastructure—that is, the cables, servers, routers, and switches that connect cyberspace. The same is true for the Supervisory Control and Data Acquisition ("SCADA") systems that run America's physical infrastructure: power, water, and communications. SCADA control functions are intranets, but are usually connected to the global Internet.").

283. *See, e.g.*, Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108–159, 117 Stat. 1952 (2003) (codified as amended in scattered Sections of 15 and 20 U.S.C.) ("FACTA"); Gramm-Leach-Bliley Financial Services Modernization Act of 1999, §§ 501–527, 15 U.S.C. §§ 6801–27 ("GLB"); Health Insurance Portability and Accountability Act of 1996, Pub. L. N. 104–191, 110 Stat. 1936 (1996) (codified as amended in scattered Sections of 18, 26, 29 and 42 U.S.C.) ("HIPAA"); FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.1–14.5 (2012) (implementing "safeguards" provisions of Gramm-Leach-Bliley); Protection of Digital Computer and Communication Systems and Networks, 10 C.F.R. § 73.54 (2012); Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007); *see also* MARK E. SCHREIBER ET AL., EDWARDS WILDMAN PALMER LLP, EVERYONE'S NIGHTMARE: PRIVACY AND DATA BREACH RISKS 25–44 (2012), http://www.acc.com/chapters/ne/loader.cfm?csModule=security/getfile&PageID=1300198 (discussing data security laws and regulations);

More recently, Congress and federal regulators have adopted a number of legislative and regulatory measures to improve transparency with respect to cyberincidents.[284] The measures most obviously designed to improve transparency are data breach notification laws. Pursuant to these laws, corporations must, under certain circumstances, disclose data breaches. As of August 2012, forty-six states[285] and the federal government[286] had

---

Stewart Baker & Melanie Schneck-Teplinsky, *Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US, in* CYBERCRIMES: A MULTIDISCIPLINARY ANALYSIS 243–48 (Sumit Ghosh & Elliot Turrini eds., 2010) (discussing financial and medical data security laws and regulations, including GLB, HIPAA, Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act"), and FACTA).

284. Such efforts are not limited to the United States. The provisions of the European Commission's draft data protection regulation now under consideration in the European Union require data controllers to "notify data breaches" and impose administrative sanctions for failure to do so. *See Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Process of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, arts. 31–32, at 11, art. 79, at 15 COM (2012) 11 final (Jan. 25, 2012), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri =COM:2012:0011:FIN:EN:PDF. Articles 31 and 32 require companies to notify their supervisory authority and affected individuals within 24 hours of discovery of a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." Article 79 provides that:

> The supervisory authority shall impose a fine up to 1,000,000 EUR or, in case of an enterprise up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently . . . does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32.

Id.

285. Every state has passed a data breach notification law except Alabama, Kentucky, New Mexico, and South Dakota. *See State Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Aug. 20, 2012) (indicating that 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted security breach notification laws); *see also State Data Breach Notification Laws*, MINTZ LEVIN, http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/statedatabreachmatrix.pdf (last updated Dec. 1, 2012) (providing a downloadable matrix of state data breach laws current as of December 2011).

286. The federal data breach notification law, codified at 42 U.S.C. § 17932, is one of several amendments to HIPAA set forth in the privacy provisions of the Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §§ 17921, 17931–40, 17951–53 (2009). The HITECH Act was embedded into the stimulus bill that President Obama signed into law on February 17, 2009. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered Sections of 6, 19, 26, and 42 U.S.C.). The HITECH

adopted such laws. SEC disclosure rules also serve to improve transparency. Specifically, the SEC Division of Corporation Finance issued staff-level guidance on October 13, 2011, at Senator John D. Rockefeller's (D-W.Va.) urging,[287] that requires companies report to the SEC "material information regarding cybersecurity risks and cyber incidents."[288] Appropriate disclosures may include, among other things, "[A d]escription of cyberincidents experienced by the [SEC] registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences . . . ."[289] Senator Rockefeller has since urged

---

Act effectively provides a safe-harbor from its breach notification requirements when protected health information ("PHI") is "secured" (e.g., encrypted using NIST-approved processes), giving covered entities and their business associates a strong incentive to maintain electronic PHI in NIST-approved encrypted form at all times. In the summer of 2009, the Department of Health and Human Services ("HHS") published an interim final "Breach Notification Rule" implementing HITECH's breach reporting requirements. *See* Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009), http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf (requiring covered entities under the HIPAA and their business associates to provide notification in the case of breaches of unsecured protected health information). *Breach Notification Final Rule Update*, U.S. DEP'T OF HEALTH AND HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html (last visited Apr. 1, 2013). The FTC issued companion breach notification regulations, FTC Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009). On January 25, 2013, HHS issued a final rule that, *inter alia*, modified the Breach Notification Rule. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566–5702 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164). Among other things, the final rule amended the definition of "breach" used in the regulations so as to "replace[] the [B]reach [N]otification [R]ule's 'harm' threshold with a more objective standard." 78 Fed. Reg. 5566, 5695. Specifically, breach notification was not required under the interim rule if a covered entity or business associate could "demonstrate that there [was] no significant risk of harm to the individual," 78 Fed. Reg. 5641, but under the final rule, a breach is presumed unless "the covered entity or business associate . . . demonstrates [through a risk assessment] that there is a low probability that the protected health information has been compromised." 78 Fed. Reg. 5695.

287. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html ("Rockefeller in May 2011 wrote to then-SEC Chairman Mary Schapiro pointing out the growing risk posed to U.S. companies by 'malicious actors' who 'attack and disrupt computer networks to steal valuable trade secrets, intellectual property, and financial and confidential information.' He asked the SEC to develop and publish guidance to clarify disclosure requirements pertaining to 'information security risk, including material information security breaches involving intellectual property or trade secrets.' ")

288. *CF Disclosure Guidance: Topic No. 2*, SEC (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

289. *Id.*

the SEC to adopt formal cybersecurity guidance. In an April 10, 2013 letter to incoming SEC Chairman, Mary Jo White, Senator Rockefeller wrote:

> While the [SEC] staff guidance has had a positive impact on the information available to investors on these matters, the disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices . . . . Investors deserve to know whether companies are effectively addressing their cybersecurity risks—just as investors should know whether companies are managing their financial and operational risks . . . . Formal guidance from the SEC on this issue will be a strong signal to the market that companies need to take their cybersecurity efforts seriously.[290]

Laws, regulations, and guidance on data breach notification arguably help the market function more efficiently by enabling it to evaluate companies in part based on their ability to keep their networks secure. The more information is available about cyberincidents and cyberthreats, the better the cybersecurity market should function, since more reliable data will help corporations more accurately calculate efficient levels of cybersecurity. Accordingly, disclosure-forcing rules are often viewed as part of a larger effort to combat what some believe to be chronic U.S. private sector underinvestment in cybersecurity.

Vulnerability mitigation has long been the cornerstone of U.S. cybersecurity policy,[291] with legislators struggling to properly incentivize corporations to improve their cyberdefenses without dampening

290. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG, (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html.http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e.

291. *See, e.g.*, WHITE HOUSE, CYBERSPACE POLICY REVIEW, *supra* note 2, at i, iii ("It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution. . . . Without major advances in the security of [the nation's digital infrastructure] systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."); *see also* Hathaway, *supra* note 156, at 78 ("[R]eal [cybersecurity] leadership requires adopting and embedding sometimes-costly security solutions into our core infrastructures and enterprises . . . ."); Press Release, Mac Thornberry, U.S. Representative, Thornberry Named Leader of New Cybersecurity Task Force (June 24, 2011), *available at* http://thornberry.house.gov/news/documentsingle.aspx?DocumentID=248853 (quoting House Majority Leader Eric Cantor (R-Va.) as saying that " '[s]trengthening our networks' security is fundamental to protecting our national and financial security, promoting economic growth, and creating jobs").

innovation.[292] The 2012 congressional session was no exception, as Senators vigorously debated the merits of legislation that would have set minimum cybersecurity standards for the private sector. Also at issue in that session was legislation designed to facilitate the flow of information—in both directions—between the private sector and the U.S. government.

A. Congressional Action (2011–2012)

A flurry of cybersecurity-related activity in both houses of Congress during the 112th Congress ultimately led to successful passage of a controversial cybersecurity bill in the House in April of 2012, but failure to pass cybersecurity legislation in the Senate during the 2012 session. Despite Congress' failure to pass cybersecurity legislation, the debate over the bills that were considered is described in some detail below as it informs current discussions about the appropriate way forward.

1. Administration Legislative Proposal

On May 12, 2011, the Administration submitted cybersecurity legislation to Congress.[293] At the core of the seven-part package were provisions giving DHS authority to regulate critical infrastructure.[294] These provisions required owners and operators of critical infrastructure to develop cybersecurity plans, the implementation of which was to be evaluated by the Secretary of DHS.[295]

2. U.S. House of Representatives

a. Republican Cybersecurity Task Force

In June of 2011, House Republicans announced the creation of a GOP-

292. There have been approximately thirty cybersecurity proposals in the House and Senate since 2009. *See* David Perera, *Congressional Cybersecurity Bill Roundup*, FIERCEGOVERNMENTIT (May 12, 2010), http://www.fiercegovernmentit.com/story/congressional-cybersecurity-bill-roundup/2010-05-12 (listing cybersecurity bills introduced during 111th Congress, i.e., January 3, 2009 through January 3, 2011); *see also* ERIC A. FISCHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: DISCUSSION OF PROPOSED REVISIONS 4–8 (2012), http://www.fas.org/sgp/crs/natsec/R42114.pdf (discussing selected cybersecurity legislative proposals considered in the 112th Congress).

293. EXEC. OFFICE OF THE PRESIDENT, OFFICE OF MGMT. & BUDGET, LAW ENFORCEMENT PROVISIONS RELATED TO COMPUTER SECURITY (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

294. *See generally* EXEC. OFFICE OF THE PRESIDENT, OFFICE OF MGMT. & BUDGET, CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT (2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-regulatory-framework-for-covered-critical-infrastructure-act.pdf.

295. *Id.* §§ 5–6.

only task force to study cybersecurity and make recommendations to House leadership.[296] The resulting task force report, issued in October of 2011, departed from the Administration's proposal in several important respects.[297] Most notably, the task force unanimously recommended adoption of voluntary cybersecurity standards tied to incentives to improve cybersecurity.[298] Representative Thornberry (R-TX), leader of the task force, subsequently explained that incentives help to "elevate [cybersecurity] in the consciousness of CEOs and businesses."[299] The task force specifically recommended that Congress consider research and development tax credits for cyberinvestments and consider whether cybersecurity insurance can help improve security.[300] The task force also recommended that Congress use federal purchasing power to improve cybersecurity by revising the Federal Acquisition Regulations to require appropriate security in all federal IT procurements.[301] At the event announcing completion of the task force report, Thornberry declared: "anybody who gets a federal grant ought to have some sort of minimum level of cybersecurity."[302] Despite differences between the Administration's legislative proposal and the task force recommendations, in December 2011, Senate Majority Leader Harry Reid (D-NV) described the House Republican cybersecurity task force recommendations as "fully consistent with our efforts."[303]

---

296. Press Release, Rep. Mac Thornberry, *supra* note 291.

297. *See, e.g.*, MAC THORNBERRY ET AL., RECOMMENDATIONS OF THE HOUSE REPUBLICAN CYBERSECURITY TASK FORCE 7–8 (2011), http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf. The task force *agreed* with the White House on "the need to simplify data-breach reporting requirements for companies, update information-security standards for government agencies, and boost recruitment of qualified cybersecurity workers." Eric Engleman, *House Republican Cybersecurity Plan Echoes Part of Obama Policy*, BLOOMBERG (Oct. 6, 2011, 12:01 AM), http://www.bloomberg.com/news/2011-10-05/house-cybersecurity-task-force-wary-of-rules-on-network-defense.html.

298. THORNBERRY ET AL., *supra* note 297, at 7–8; Engleman, *supra* note 297 (explaining that the report also recommended that Congress facilitate the creation of a non-government clearinghouse for information-sharing among businesses and the government). Task force leader Rep. Thornberry also noted that about fifty outdated laws related to cybersecurity need to be revised and he noted that "basic hygiene" steps could eliminate the majority of malware. *Id.*

299. Zach Rausnitz, *House Cybersecurity Task Force Suggest Incentives, Info-Sharing*, FIERCE HOMELAND SEC. (Oct. 12, 2011), http://www.fiercehomelandsecurity.com/story/house-cybersecurity-task-force-suggests-incentives-info-sharing/2011-10-12#ixzz2EnMEIhif.

300. THORNBERRY ET AL., *supra* note 297, at 8.

301. *See id.* at 19.

302. Rausnitz, *supra* note 299.

303. Gautham Nagesh, *Reid says Senate will take up cybersecurity bill next year*, THE HILL (Nov. 17, 2011, 11:52 AM), 194245-senate-will-take-up-cybersecurity-bill-

b. CISPA

Ultimately, the House did not pass legislation based on the recommendations of its cybersecurity task force. Instead, on April 26, 2012, after nearly seven hours of debate,[304] the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act ("CISPA") of 2012,[305] a highly controversial bill that, according to legislative sponsors, was designed to address the Chinese and Russian cyberespionage threat[306] and protect critical infrastructure.[307]

The purpose of CISPA was to remove legal obstacles to information sharing[308] between private sector companies and the U.S. government in two ways. First, CISPA was drafted to give the intelligence community the authority to share cyber threat intelligence, including classified intelligence, with certain private-sector entities under certain conditions.[309]

---

next-year.

304. Declan McCullagh, *How CISPA Would Affect You (faq)*, CNET (Apr. 27, 2012, 4:00 AM), http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/.

305. H.R. 3523, 112th Cong. (2012). CISPA is also known as the Rogers-Ruppersberger bill after Mike Rogers (R-Mich.) and Dutch Ruppersberger (D-Md.), the chairman and the ranking member of the House Permanent Select Committee on Intelligence ("HPSCI"), respectively.

306. *See* Declan McCullagh, *House Passes CISPA Internet Surveillance Bill*, ZDNET (Apr. 27, 2012, 5:00 AM), http://www.zdnet.com/news/house-passes-cispa-internet-surveillance-bill/6360341 ("[HPSCI Chairman Rogers said that CISPA is] needed to stop the Chinese government from stealing our stuff [and that the Chinese are] stealing the value and prosperity of America."); Press Release, Rep. Mike Rogers, Co-Sponsors Top 100 for the Rogers-Ruppersberger Bipartisan Cyber Bill (Mar. 29, 2012), *available at* http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=287920 ("Every day U.S. businesses are targeted by nation-state actors like China for cyber exploitation and theft . . . . This consistent and extensive cyber looting results in huge losses of valuable intellectual property, sensitive information, and American jobs. The broad base of support for this bill shows that Congress recognizes the urgent need to help our private sector better defend itself from these insidious attacks . . . .").

307. Press Release, Rep. Mike Rogers, *supra* note 306 (quoting HPSCI Ranking Member C.A. Dutch Ruppersberger) ("Without important, immediate changes to American cybersecurity policy, I believe our country will continue to be at risk for a catastrophic attack to our nation's vital networks—networks that power our homes, provide our clean water or maintain the other critical services we use every day. This small but important piece of legislation is a decisive first step to tackle the cyber threats we face.").

308. James A. Lewis, *Code Red*, FOREIGN POL'Y (Aug. 1, 2012), http://www.foreignpolicy.com/articles/2012/08/01/code_red ("[Information to be shared] can include 'signatures' and other cyberthreat indicators, such as intelligence information, reports of successful penetrations, and information on the identities or network addresses of the 'attacking computers . . . .' ").

309. *See* H.R. 3523 § 1104(a)(1) (amending the National Security Act of 1947 to require the Director of National Intelligence "to establish procedures to allow elements of the intelligence community to share cyber threat intelligence [including classified

Second, CISPA was designed to encourage businesses to voluntarily share cyberthreat information with the government by offering a variety of protections, including exemptions from liability;[310] limitations on government disclosure of shared information, including a Freedom of Information Act ("FOIA") exemption;[311] and prohibition on government use of shared cyberthreat information for regulatory purposes.[312]

Supporters of CISPA describe it as an "information sharing" bill. They say it "helps the private sector defend itself from advanced cyber threats, without imposing any new federal regulations or unfunded private sector mandates, and contains protections for privacy and civil liberties."[313] Opponents include not only an array of privacy and civil liberties advocates, who claim that CISPA will make it easier for the federal government to access personal information,[314] but also those who see the

---

intelligence] with private-sector entities"); *id.* § 1104(a)(2)(A) (classified cyber threat intelligence may only be shared with "certified entities" or persons with "an appropriate security clearance"); *id.* § 1104(a)(2)(C) ("[C]lassified cyber threat intelligence may only be . . . used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure."); *id.* §1104(a)(3)(B) (providing authority to "grant a security clearance on a temporary or permanent basis to a certified entity" and grant "approval to use appropriate facilities"). Taken together, these provisions allow the government to share classified threat information with businesses under certain specific conditions. For example, businesses receiving classified threat information may need security clearances for personnel and technical, administrative, and procedural safeguards to handle classified information.

310. *Id.* § 1104(b)(4)(A) ("No civil or criminal cause of action shall lie or be maintained in Federal or State court against a [cybersecurity provider or certain other designated entities] acting in good faith for using cybersecurity systems to identify or obtain cyber threat information or for sharing such information in accordance with this section . . . .").

311. *Id.* § 1104(b)(3)(C)(i) (providing that cyberthreat information shared with the federal government "shall be exempt from disclosure under section 552 of title 5, United States Code [i.e., FOIA]"); *id.* §1104(b)(3)(C)(ii) (providing that cyberthreat information shared with the federal government "shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information").

312. *Id.* §1104(b)(3)(C)(iii).

313. Press Release, Rep. Mike Rogers, *supra* note 306.

314. *See* Chloe Albanesius, *Internet Groups Launch Anti-CISPA Protest*, PC MAG. (Apr. 16, 2012, 12:28 PM), http://www.pcmag.com/article2/0,2817,2403080,00.asp; *see also* Declan McCullagh, *Advocacy Group Flip-Flops Twice Over CISPA Surveillance Bill*, CNET (Apr. 25, 2012, 10:53 PM), http://news.cnet.com/8301-31921_3-57421624-281/advocacy-group-flip-flops-twice-over-cispa-surveillance-bill/ (discussing positions taken by the Center for Democracy and Technology, the American Civil Liberties Union, and the Electronic Frontier Foundation); Greg Nojeim, Jim Dempsey, & Leslie Harris, *A Recap of Months of CDT Advocacy on CISPA*, CTR. FOR DEMOCRACY & TECH. (Apr. 26, 2012), https://www.cdt.org/blogs/2604recapping-state-play-cispa ("Since CISPA was introduced, CDT has consistently said the bill has three critical civil liberties problems . . . . The first is that CISPA permits unfettered sharing of private communication with

bill as doing little to advance cybersecurity.[315] As one cybersecurity expert bluntly stated: "sharing information is a feeble response to a serious threat."[316] President Obama was equally decisive—although somewhat more reserved—when he weighed in on the issue in a July 2012 op-ed, stating, "Simply sharing more information is not enough. Ultimately, this is about security gaps that have to be filled."[317]

CISPA was an enormously controversial bill.[318] Although the bill's sponsors amended CISPA just days before it passed the House ostensibly to address privacy and civil liberties concerns, several of the most controversial provisions in the bill remained untouched. One such provision is § 1104(b)(1)(B) which provides as follows:

> Notwithstanding any other provision of law, a self-protected entity[319] may, for cybersecurity purposes—
>
> (i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and
>
> (ii) share such cyber threat information with any other entity, including the Federal Government.[320]

CISPA critics maintain that the phrase "notwithstanding any other provision of law" allows the private sector to share threat information with the government regardless of existing federal and state laws—including

---

the government; second, it permits that sharing to go to any agency including the super-secret NSA; and third, it permits the government to use this information for purposes wholly unrelated to cybersecurity. On these grounds we oppose CISPA.").

315. Mac Thornberry, *Cybersecurity Needs Our Full Attention*, POLITICO (Apr. 25, 2012, 9:24 PM), http://www.politico.com/news/stories/0412/75604.html #ixzz2EntrTr5D (supporting CISPA, but noting the most prominent criticism is that CISPA "does not go far enough").

316. Lewis, *supra* note 308.

317. Obama, *supra* note 100.

318. The controversy over CISPA stemmed in part from its substantive provisions and in part from comparisons—some unwarranted—of CISPA to the Stop Online Privacy Act ("SOPA"), H.R. 3261, and PROTECT IP Act ("PIPA"), S.B. 968, legislation that was roundly condemned in the technology community months before. *See* Violet Blue, *Say 'Hello' to CISPA, It Will Remind You of SOPA*, CNET (Apr. 13, 2012, 7:35 AM), http://news.cnet.com/8301-1023_3-57413627-93/say-hello-to-cispa-it-will-remind-you-of-sopa/; Rebecca Greenfield, *Why CISPA is Worse Than SOPA*, THE ATLANTIC WIRE (Apr. 27, 2012), http://www.theatlanticwire.com /technology/2012/04/why-cispa-worse-sopa/51638/; Megha Rajagopalan, *Is CISPA SOPA 2.0? We Explain the Cybersecurity Bill*, PROPUBLICA (Apr. 26, 2012, 11:16 AM), http://www.propublica.org/article/is-cipsa-sopa-20-we-explain-the-cybersecurity-bill.

319. A "self-protected entity" is "an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself." Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. § 1104(h)(12).

320. *Id.* § 1104(b)(1)(B).

laws such as the Electronic Communications Privacy Act[321]—some of which specifically limit such sharing in order to protect information privacy and civil liberties. Moreover, critics maintain that use of such sweeping language could have "unforeseen consequences."[322]

Another highly controversial aspect of CISPA—and one that was not addressed by amendments—was that it permits the private sector to share cyberthreat information directly with the National Security Agency ("NSA").[323] Rhetoric began to fly when this provision was interpreted in some circles as raising the specter of government surveillance. Representative Jared Polis (D-Co) argued: "Allowing the military and NSA to spy on Americans on American soil goes against every principle this country was founded on."[324] HSPCI Chairman Rogers defended CISPA, saying: "There is no government surveillance, none, not any in this bill."[325] In fact, CISPA does not include a formal grant of surveillance authority to NSA, but the bill arguably "usher[s] in a new era of information sharing between companies and government agencies—with limited oversight and privacy safeguards."[326] The Administration took the position that CISPA "effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres."[327]

---

321. 18 U.S.C. §§ 2511–22 (2012).

322. RICHARD S. BETH, CONG. RESEARCH SERV., RS 20617, HOW BILLS AMEND STATUTES 1–2 (2003), http://assets.opencrs.com/rpts/RS20617_20030804.pdf ("[A] bill may preface new provisions being added to law with such a phrase as, 'notwithstanding any other provision of law.' Such a phrase tends to imply that the new language is intended to supersede any conflicting provisions of previous law. This broad phrase, however, does not specify which provisions it is meant to refer to, and may therefore have unforeseen consequences for both existing and future laws.").

323. House leadership did not allow for amendments on this issue. The Center for Democracy and Technology ("CDT"), which had vigorously opposed CISPA, came to an informal understanding with the House Intelligence Committee that, in return for CDT's willingness not to oppose CISPA moving forward, the House would consider amendments on what CDT considered to be two major privacy and civil liberties issues in CISPA—"the flow of internet data directly to the NSA and the use of information for purposes unrelated to cybersecurity . . . ." When the House leadership subsequently blocked amendments on both issues, CDT reasserted its opposition to CISPA. *See* Press Release, Ctr. for Democracy & Tech., CDT Opposes CISPA Going Forward (Apr. 25, 2012), *available at* https://www.cdt.org/prstatement/cdt-opposes-cispa-going-forward.

324. McCullagh, *supra* note 306.

325. Josh Smith, *Bucking Veto Threat, House OKs CISPA Cybersecurity Information-Sharing Bill*, NAT'L J. (Apr. 26, 2012, 7:02 PM), http://www.nationaljournal.com/tech/bucking-veto-threat-house-oks-cispa-cybersecurity-information-sharing-bill-20120426.

326. McCullagh, *supra* note 304.

327. *Id.*

Other controversial provisions of CISPA were amended before its passage. For example, after critics lambasted the bill's original language allowing the government to use information shared under CISPA for "any lawful purpose," the bill was amended to limit government use and retention of shared information to five enumerated purposes: (1) cybersecurity;[328] (2) investigation and prosecution of cybersecurity crimes; (3) protection of individuals from the danger of death or serious bodily harm and investigation and prosecution of crimes involving such dangers; (4) protection of minors from harm and/or exploitation (including sexual exploitation, kidnapping, and trafficking); and (5) protection of U.S. national security.[329] While acknowledging that these changes were a step in the right direction, critics nonetheless expressed concern that the amended language continued to permit "information shared under CISPA [to] be used in criminal proceedings against individuals [even though] it can be collected without any Fourth Amendment considerations."[330]

CISPA supporters were quick to note that the bill does not obligate private sector companies to share information with the government; participation in information sharing is entirely voluntary.[331] But critics contended that "the cost of this information sharing—in terms of privacy lost and civil liberties violated—is borne by individual customers and Internet users. For them, nothing about CISPA is voluntary[,] and for them there is no recourse," because CISPA affords broad liability protection to companies who share information and exempts shared information from FOIA.[332]

The Obama administration threatened to veto CISPA unless it ramped up protections for critical infrastructure and privacy protections,[333] but much

328. The definition of "cybersecurity" was itself limited by the amendments.

329. Cyber Intelligence Sharing and Protection Act, H.R. 3523 112th Cong. § 1104(c)(1) (2012).

330. Alexander Furnas, *Can Last-Minute Amendments Redeem the Troubling Cybersecurity Bill?*, THE ATLANTIC (Apr. 25, 2012, 6:45 PM), http://www.theatlantic.com/technology/archive/2012/04/can-last-minute-amendments-redeem-the-troubling-cybersecurity-bill/256372/. CISPA's definition of "cyber threat intelligence" also was amended to address criticisms of over-breadth, but remains controversial. *See* Anjali Dalal, *Why the Cyber Intelligence Sharing and Protection Act (CISPA) Is Not the Solution to U.S. Cyber Attack Fears*, JUSTIA (May 2, 2012), http://verdict.justia.com/2012/05/02/why-the-cyber-intelligence-sharing-and-protection-act-cispa-is-not-the-solution-to-u-s-cyber-attack-fears (detailing how CISPA may circumvent the Fourth Amendment).

331. David Inserra, *CISPA Is Ready for Primetime*, THE FOUNDRY (Apr. 25, 2012, 6:30 PM), http://blog.heritage.org/2012/04/25/cispa-is-ready-for-prime-time/.

332. Furnas, *supra* note 330.

333. Andrew Couts, *CISPA Cybersecurity Bill Passes House 248 to 168*, DIGITAL TRENDS (Apr. 26, 2012), http://www.digitaltrends.com/web/cispa-cybersecurity-bill-passes-house-248-to-168/#ixzz2DuTt6QBq.

of the technology industry supported CISPA,[334] apparently in hopes that Congress would otherwise remain hands-off with respect to cybersecurity.[335]

One cybersecurity expert summarized the CISPA saga as follows:

> Congress knows that weak cybersecurity endangers the country—and that America is dangerously unprepared—but it cannot muster a majority to support serious defensive measures. The same forces that have kept Capitol Hill in gridlock on many important issues have also blocked effective cybersecurity legislation. That said, Congress does not want to be in the position, after the inevitable cyberdisruption, of having to say it knew but did nothing. The political solution to gridlock is to pass weak legislation and pretend it will work. This is the CISPA story.[336]

3. U.S. Senate

The Senate ultimately failed to pass cybersecurity legislation in 2012, however a number of bills made their way through the Senate, the most important of which were: (1) the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act ("SECURE-IT") of 2012;[337] (2) the Cybersecurity Act of 2012 ("CSA");[338] and (3) the Revised Cybersecurity Act of 2012.

a. SECURE-IT Act

The SECURE-IT Act of 2012, sponsored by Senator McCain and other Republicans, was an information-sharing bill. It enabled private sector "cyberthreat information" sharing with the government, including NSA. The bill was first introduced in February and was re-introduced in June with changes designed to address criticisms of the original bill. According to its sponsors, the Act "recognizes industry's central role in protecting cyber networks and provides it the liability protection it needs to share real-time cyber threat information that is necessary to combat cyber attacks."[339]

---

334. *H.R. 3523 Letters of Support*, H. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/hr-3523-letters-support (last visited Apr. 1, 2013) (listing numerous letters of support from trade associations such as BSA, Business Roundtable, and the U.S. Chamber of Commerce as well as individual companies such as AT&T, Boeing, Facebook, Lockheed Martin, Microsoft, Oracle, Symantec, and Verizon).

335. Lewis, *supra* note 308 ("One powerful motive for [CISPA's] passage, as a House member privately told companies, was that it would 'help protect you from regulation.' ").

336. *Id.*

337. Introduced as S. 2151 on March 1, 2012; re-introduced as S. 3342 on June 27, 2012.

338. Introduced as S. 2105 on February 14, 2012; re-introduced as S. 3414 on July 19, 2012.

339. Press Release, Senator John McCain, Senators Renew Push to Strengthen

Civil liberties groups were highly critical of both the original and re-introduced bills,[340] asserting, for example, that the legislation's vague definition of "cyberthreat information" could lead to government invasions of personal privacy.[341] More fundamentally, civil libertarians labeled SECURE-IT a "backdoor wiretap bill."[342] They claimed that despite modifications of some of the bill's provisions:

> SECURE IT still allows far too much information to flow to the government, allows information to flow directly from companies in the private sector to the NSA and other elements of the Department of Defense, and allows shared cyber threat information to be used for non-cybersecurity purposes such as national security and law enforcement. Much of this information would otherwise be protected from government access by the Fourth Amendment warrant requirement. Bypassing the warrant requirement to facilitate intelligence and law enforcement investigative activity effectively turns cybersecurity information sharing into a back-door wiretap. The incremental, pro-privacy changes made to SECURE IT [when it was re-introduced in June] do not overcome these fundamental flaws in the legislation.[343]

The SECURE-IT Act stood in stark contrast to the CSA (described in more detail below). SECURE-IT took a market-based, rather than regulatory, approach and gave the federal government no new regulatory authority with respect to cybersecurity standards. In the House, Reps. Mary Bono Mack (R-Cal.) and Marsha Blackburn (R-Tenn.) introduced legislation that mirrors SECURE-IT, with only minor changes.[344]

b. Cybersecurity Act

CSA was originally introduced in February of 2012 by Senators

---

Cybersecurity (June 27, 2012), *available at* http://www.mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=2ed8acb7-cb2a-043e-7bb4-26766aaa2b5b.

340. Greg Nojeim & Jon Miller, *SECURE-IT: Building a Better Back-Door Wiretap*, CTR. FOR DEMOCRACY & TECH. (July 30, 2012), https://www.cdt.org/blogs/greg-nojeim/3007secure-it-building-better-back-door-wiretap (outlining what CDT viewed as "fundamental flaws" in SECURE-IT); Letter from Coalition in Opposition of SECURE-IT to U.S. Senators (May 14, 2012), https://www.cdt.org/files/pdfs/SecureIT_Coalition_Letter.pdf.

341. Nojeim & Miller, *supra* note 340 (outlining what CDT viewed as "fundamental flaws" in SECURE-IT).

342. *Id.*

343. *Id.*

344. Josh Smith, *Bono Mack, Blackburn Introduce Industry-Friendly Cyber Bill*, NAT'L JOURNAL (Mar. 27, 2012, 11:14 AM), http://www.nationaljournal.com/blogs/techdailydose/2012/03/bono-mack-blackburn-introduce-industry-friendly-cyber-bill-27.

Lieberman, Collins, Rockefeller, and Feinstein in response to Majority Leader Reid's instruction that all committees of jurisdiction work together to produce a single piece of legislation.[345] In its original form, CSA (1) authorized DHS to establish baseline mandatory cybersecurity performance requirements for systems in critical infrastructure sectors; and (2) included information-sharing provisions to facilitate private sector sharing of cyberthreat information with other private sector companies and with the government.[346]

CSA's opponents—including many Republicans and industry groups—tendered the standard arguments against cybersecurity regulation, arguing that it would be costly, ineffective, and hamper innovation.[347] Industry opponents also likely harbored concern (albeit rarely expressed) that establishing cybersecurity standards—even minimum baselines standards—would raise the specter of potential tort liability for losses caused by a corporation's failure to meet those standards.

One of the most commonly heard refrains from CSA opponents was that the bill would encourage a culture not of "security," but of "compliance." The Business Roundtable, an association of CEOs of major U.S. companies, stated: "[CSA] would lead to static, prescriptive regulations that do not address dynamic cybersecurity risks and would force companies to shift scarce resources from security to compliance."[348] The Business Roundtable maintained that CSA favored "burdensome and ineffective 'check-the-box' security approaches over sophisticated management of shared cyber risks."[349] Echoing these sentiments, the Telecommunication Industry Association, the lead industry association representing manufacturers and suppliers of global networks, wrote:

> [I]ndustry's primary concern with transitioning to a mandatory regulatory regime . . . . is that imposing rigid regulatory requirements—requirements that by their nature will be unable to keep up with rapidly

345. *Cybersecurity*, U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOV'T AFF., http://www.hsgac.senate.gov/issues/cybersecurity (last visited Apr. 1, 2013).

346. *See* Cybersecurity Act of 2012, S. 2105 §§ 105, 701–08 (2012).

347. *See* David Inserra, *Cybersecurity Executive Order Touts More Regulation as the Solution*, THE FOUNDRY (Nov. 2, 2012, 1:58 PM), http://blog.heritage.org/2012/11/02/cybersecurity-executive-order-touts-more-regulation-as-the-solution/ ("[R]egulations hinder innovation. Since companies will try to meet outdated cybersecurity regulations, cybersecurity companies will focus on meeting this demand. However, time spent meeting this demand for older cybersecurity approaches is time not being spent innovating ways to fight newer threats.").

348. Letter from Ajay Banga, Chair, Info. & Tech. Comm., Bus. Roundtable, to Harry Reid & Mitch McConnell, U.S. Senators (July 31, 2012), *available at* http://businessroundtable.org/news-center/business-roundtable-letter-on-the-revised-cybersecurity-act-of-2012/.

349. *Id.*

> evolving technologies and threats—would require industry to focus on obsolete security requirements rather than facing the actual threat at hand, effectively making systems *less* secure. Instead, the key to improving the cybersecurity of critical infrastructure is to strengthen the broader cyber ecosystem that enables rapid information sharing, enhances public private partnerships, and provides sufficient investment to address current and emerging threats.[350]

Meanwhile, proponents of CSA viewed the bill as a basic—and long overdue—effort to provide a necessary security framework for private sector companies, particularly those that control critical infrastructure.[351] Under the CSA,

> Company CEOs would only need to certify once a year that they had taken steps to secure their networks, using measurable outcome-based guidelines. DHS would not prescribe how they should do this, but simply define outcomes that a company could then use any technology or technique to achieve. This was very light regulation, but for some it was still too much.[352]

c. Revised Cybersecurity Act

On July 19, 2012, in what was ultimately an unsuccessful attempt to secure Senate passage of their cybersecurity legislation, Senators Lieberman and Collins introduced a revised version of their omnibus cybersecurity bill ("Revised Cybersecurity Act") designed to address Republican concerns. The compromise bill, which the Obama Administration supported, included *voluntary* cybersecurity standards for critical infrastructure,[353] information-sharing provisions,[354] and substantial

350. TELECOMMS. INDUS. ASS'N, *supra* note 282; *see* Inserra, *supra* note 347 ("[R]egulations create a false sense of security and an attitude of compliance. The private sector would follow the regulations and do little more. After all, if it follows the regulations, the government has declared that the private sector is doing cybersecurity right. This will give the private sector the wrong incentive. Instead of promoting the adoption of the most appropriate cybersecurity system, regulations merely encourage the private sector to meet the outdated standards.").

351. CSA reflects the view espoused by some experts that federal government action is necessary to secure the Internet's infrastructure. *See, e.g.*, SPADE, *supra* note 23, at 36 ("The biggest step the federal government can take is to secure the Internet's infrastructure . . . . If the government intends to use the commercial sector for IT, industry security must be federally regulated."). Colonel Spade takes the argument even further, arguing that "SCADA systems must be disconnected from the Internet." In his view, critical infrastructure should then be included in a "federally secured network," which would "allow national utilities to remain linked with greatly reduced vulnerability to CNE [i.e., cyber network exploitation]." *Id.*

352. Lewis, *supra* note 308.

353. *See* Cybersecurity Act of 2012, S. 3414, 112th Cong. § 103; *see also* Jonathan G. Cederbaum et al., *Senate to Consider Compromise Cybersecurity Legislation*,

civil liberties protections.[355]

First, the Revised Cybersecurity Act provided for voluntary standards. To encourage CI owners and operators to adopt the standards, the bill offered an array of incentives. The incentives included liability protection from any punitive damages arising out of a cybersecurity incident if the CI owner/operator was substantially in compliance with the standards at the time of the incident; priority technical assistance for response to cyber threats; and potential access to classified cyberthreat information.[356]

Second, the Revised Cybersecurity Act included revised information-sharing provisions.[357] These provisions required the creation of a federal cybersecurity information exchange led by a civilian agency,[358] and limited the sharing of private-sector provided cyberthreat information with other Federal agencies. In this vein, the bill allows disclosure of cyberthreat indicators to, and use of those indicators by, law enforcement only for specific purposes.[359] The bill also provides liability protection for private sector actors who share information with the government in "good faith" and without "gross negligence."[360]

Critics of the compromise bill described a number of concerns in addition to those typically expressed in prior debates over cybersecurity standards (i.e., cost, hindered innovation, "compliance" over "security," etc.). For example, one critic suggested that "the government will withhold cyber threat and vulnerability information from those private sector actors who do not adopt the [voluntary] standards"[361] and wrote:

WILMERHALE (July 23, 2012), http://wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737418914.

354. *See* S. 3414 §§ 701–08.

355. *See, e.g.*, *id.* § 201 (amending the Federal Information Security Management Act to include the civil liberties protections set forth in §§ 3553(b)(1)(G), 3553(e)(2)(A)(ii), and 3554(b)); *id.* § 301 (amending the Homeland Security Act of 2002 by adding Sections 242(d)(4) and 243(a)(4)); *id.* §§ 704(g)(3)–(6). For a detailed analysis of the provisions of the Revised Cybersecurity Act, see Cederbaum et al., *supra* note 353.

356. *See* SENATE COMM. ON HOMELAND SEC. & GOVERNMENTAL AFF., THE REVISED CYBERSECURITY ACT OF 2012 S. 3414 (INTRODUCED JULY 19 2012) (2012), http://www.hsgac.senate.gov/download/cybersecurity-act-of-2012_-revision-two-page-summary; *see also* Paul Rosenzweig, *Thoughts About the Revised Lieberman-Collins Cybersecurity Bill*, LAWFARE (July 21, 2012, 11:20 AM), http://www.lawfareblog.com/2012/07/thoughts-about-the-revised-lieberman-collins-cybersecurity-bill/.

357. S. 3414 §§ 701–08.

358. *Id.* § 703.

359. *Id.* § 704(g)(2).

360. *Id.* § 706(b), (g).

361. Rosenzweig, *supra* note 356.

> It is at least reasonable to ask whether this is the right carrot. Should the government be in the position of denying government threat information to critical infrastructure owners who choose not to adopt the voluntary standards (especially if that decision may be for justifiable business reasons of cost). If the infrastructure in question is truly "critical" it is in America's collective interest to protect them as much as we can. Denying them the informational tools to do so because they don't follow the government's lead may be cutting off our nose to spite our own face.[362]

Another criticism was that the bill did not sufficiently protect companies against liability. Although the bill protects companies from punitive damages if they comply with the standards, one legal scholar claimed that the protections were of little value saying, "I would have argued that even in the absence of an explicit liability protection[,] any company that adopted government approved cybersecurity standards and could show their compliance with them would be immune from punitive damages."[363]

Cybersecurity expert James Lewis criticized the compromise bill for a more fundamental reason. According to Lewis, the bill "simply translates the status quo into legislation—a status quo we all know is inadequate."[364] Lewis explains that the bill "relies on voluntary action—for everyone, regardless of their importance to national security. But what everyone does now is entirely voluntary, and more of the same will not improve security."[365] According to Lewis:

> [The bill] continues the overreliance on information sharing, accompanied by complicated protections to assuage the privacy community. Regulatory agencies can make cybersecurity standards mandatory to the limits of their existing authorities . . . . The bill offers weak incentives for companies to certify that their networks are secure . . . . [and f]ew companies are likely to certify themselves because the incentives in the bill don't compensate for the regulatory risk this creates.[366]

Notwithstanding these criticisms, the White House and many Senators lent their support to the bill. In an unusual move, President Obama signed a July 19, 2012, *Wall Street Journal* op-ed urging the Senate to pass the compromise bill. He argued:

---

362. *Id.*
363. *Id.*
364. Lewis, *supra* note 308.
365. *Id.*
366. *Id.*

> The American people deserve to know that companies running our critical infrastructure meet basic, commonsense cybersecurity standards, just as they already meet other security requirements. Nuclear power plants must have fences and defenses to thwart a terrorist attack. Water treatment plants must test their water regularly for contaminants. Airplanes must have secure cockpit doors. We all understand the need for these kinds of physical security measures. It would be the height of irresponsibility to leave a digital backdoor wide open to our cyber adversaries.[367]

It is important to note that the Senate's compromise bill embraced a voluntary, incentives-based system; precisely the system that the Chamber of Commerce proposed in their March 2011 White Paper and that the House task force endorsed in October 2011.[368] Even so, on August 2, 2012, just weeks before the 2012 election, Senate Republicans blocked the compromise legislation from coming to a vote after "a handful of business lobbying groups and trade associations, most notably the United States Chamber of Commerce," opposed "voluntary" standards.[369] CSA's supporters failed (by a vote of 52-46) to get the sixty votes needed to end debate on the filibustered bill.[370]

On October 13, 2012, just days after then-Defense Secretary's Panetta's "cyber 9/11" speech, Senate Majority Leader Harry Reid vowed to bring the stalled legislation back for Senate consideration during the lame duck session.[371] On November 14, the Senate once again failed to advance the legislation, this time by a vote of 51-47.[372]

---

367. Obama, *supra* note 100.

368. THORNBERRY ET AL., *supra* note 297, at 7–8 ("Congress should encourage participation in the development of voluntary cybersecurity standards and guidance through non-regulatory agencies such as [NIST], to help the private sector improve security. These standards should be developed by a public-private partnership, focus on security best practices, and remain technology-neutral as much as possible. Additionally, the public-private partnership should evaluate which incentives or strategies would increase the adoption of successful security best practices. An example would include varying degrees of liability protections afforded to companies that voluntarily implement the enhanced security practices.").

369. Letter from John D. Rockefeller IV, U.S. Senator, Chairman, Comm. on Commerce, Sci. & Transp., to Virginia M. Rometty, President & C.E.O., IBM (Sept. 19, 2012), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5.

370. Sarah Orrick, *Cybersecurity Bill Blocked by Senate Filibuster*, CONG. DIG. (Aug. 3, 2012), http://congressionaldigest.com/cybersecurity-bill-blocked-by-senate-filibuster/.

371. Ben Geman, *Reid Vows Fresh Effort to Pass Stalled Cybersecurity Bill in November*, THE HILL (Oct. 13, 2012, 2:38 PM), http://thehill.com/blogs/hillicon-valley/technology/261891-reid-vows-fresh-bid-to-pass-stalled-cybersecurity-bill.

372. *Bill Summary & Status, 112th Congress (2011-2012), S. 3414*, LIBR. OF CONG. http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.3414: (last visited Apr. 2, 2013).

B. Rockefeller Letter

On September 19, 2012, just weeks after comprehensive cybersecurity legislation was first blocked in the Senate, Senator Rockefeller sent an "unprecedented"[373] letter directly to the CEO of each of the Fortune 500 companies seeking their views on cybersecurity "without the filter of Beltway lobbyists."[374] Senator Rockefeller posed the following eight questions seeking detailed information on corporate cybersecurity practices:[375]

1. Has your company adopted a set of best practices to address its cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.
4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?
5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?
6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?
7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?
8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

Then (in what appears to have been a thinly veiled reference to passage

373. *See* Catherine Dunn, *Ex-IBM Privacy Officer on Preparing for the Future of Cybersecurity*, LAW.COM (Nov. 30, 2012), http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202578672642&ExIBM_Privacy_Officer_on_Preparing_for_the_Future_of_Cybersecurity&slreturn=20130122101602 (quoting Harriet Pearson, former IBM Chief Privacy Officer and now-partner at Hogan Lovells, describing Rockefeller's letter as "unprecedented").

374. Letter from John D. Rockefeller IV to Virginia M. Rometty, *supra* note 369.

375. *Id.*

of the Patriot Act after 9/11) Senator Rockefeller wrote that the approach taken in the compromise bill "strikes me as one that companies would want to have codified in statute, rather than risking reactive and overly prescriptive legislation following a cyberdisaster."[376] Yet,

> [m]ost observers believe that the United States will only get effective cybersecurity legislation after there has been a crisis and that the country will then overreact, trampling privacy and putting in place rigid requirements. No one on the Hill wants this outcome, but it may be unavoidable. The fate of cybersecurity legislation is symptomatic of a larger political crisis. Congress knows there is a problem, but cannot agree on a fix.[377]

In the absence of a legislative fix in the 2011–2012 session, Senator Rockefeller and others urged President Obama to address cybersecurity through an Executive Order, while many Republicans, including Senator Collins, cautioned the President against doing so.[378]

C. *Executive Order*

> *Whether these [cybersecurity] bills become law or not, the task of finding new, effective ways to secure the country's infrastructure and networks will now revert to the executive branch.*[379]
> *- James A. Lewis, CSIS*

As early as August 2012, press reports suggested that the White House, frustrated by Congress' failure to act on cybersecurity, had begun to entertain the idea of taking executive action.[380] The White House focused its efforts on critical infrastructure protection, the most controversial part of the comprehensive cybersecurity legislation that failed in the Senate, recognizing, of course, that limits on executive authority would constrain its ability to fully implement its policy vision through executive action.[381]

---

376. *Id.*

377. Lewis, *supra* note 308.

378. Eric Chabrow, *'We Can't Wait' for Cybersecurity: Divisions Surface Among Cybersecurity Act Backers*, BANK INFO SECURITY (Sept. 10, 2012), http://www.bankinfosecurity.com/blogs/we-cant-wait-for-cybersecurity-p-1352 ("[A]n Executive Order should not be a substitute for legislative action . . . . An executive order could send the unintended signal that congressional action is not urgently needed.").

379. Lewis, *supra* note 308.

380. Suzanne Kelly, *President Mulling Executive Order to Fill Cybersecurity Gap*, CNN (Aug. 9, 2012, 4:49 PM), http://security.blogs.cnn.com/2012/08/09/president-mulling-executive-order-to-fill-cybersecurity-gap/.

381. *See, e.g.*, CTR. FOR ENERGY & ENVTL. SEC., UNIV. OF COLO. L. SCH., THE BOUNDARIES OF EXECUTIVE AUTHORITY: USING EXECUTIVE ORDERS TO IMPLEMENT FEDERAL CLIMATE CHANGE POLICY 15–21, http://cospl.coalliance.org

Just six weeks after Senate Republicans first blocked comprehensive cybersecurity legislation, the Administration had completed an initial draft of its cybersecurity Executive Order ("EO").[382] A revised draft, dated November 21, surfaced shortly after Senate Republicans blocked passage of compromise cybersecurity legislation on November 14, 2012 during the lame duck session.[383]

Although DHS Secretary Janet Napolitano suggested that the Administration's cybersecurity EO was "close to completion" in late September,[384] the final EO was not signed until February 12, 2013.[385] Some theorized that the Administration was working to "get it right" by reaching out to stakeholders for input. Indeed, according to a White House spokeswoman, by the end of November, "The National Security Staff ha[d] held over 30 meetings with industry, think tanks, and privacy groups, meeting directly with over 200 companies and trade organizations representing over 6,000 companies that generate over $7 trillion in economic activity and employ more than 15 million people."[386] Others conjectured that the *threat* of an EO dealing only with the critical infrastructure problem could open the door for legislative movement on the previously-stalled comprehensive cybersecurity bill.[387] Still others thought

---

/fedora/repository/co:5359 (discussing sources of authority for executive orders); *see also* Brian Prince, *Obama Administration in Talks to Draft Cyber-Security Executive Order*, EWEEK (Nov. 27, 2012), http://www.eweek.com/servers/obama-administration-in-talks-to-draft-cyber-security-executive-order/ (discussing constraints on what executive orders can accomplish).

382. The Administration's draft Executive Order is not to be confused with the administration's Presidential Decision Directive, PDD-20, signed in October or with the draft Presidential Directive on Critical Infrastructure Protection which is designed to update HSPD-7. *See* Nakashima, *supra* note 271. Although initial media reports suggested that a draft of the Administration's Executive Order had been leaked in mid-September, the leaked document was the Presidential Directive updating HSPD-7. *See* Mike Masnick, *LEAKED! Here's the White House's Draft Cybersecurity Executive Order*, TECHDIRT (Sept. 14, 2012, 8:23 PM), http://www.techdirt.com/articles/20120914/19280020390/leaked-heres-white-houses-draft-cybersecurity-executive-order.shtml.

383. Draft Exec. Order, Improving Critical Infrastructure Cybersecurity (Nov. 21 2012), http://www.lawfareblog.com/wp-content/uploads/2012/11/White-House-Draft-Executive-Order-Dated-11-21-12.pdf [hereinafter Draft Exec. Order].

384. *Sen. Rockefeller Asks Fortune 500 CEOs for Cybersecurity Best Practices*, HOMELAND SEC. NEWS WIRE (Oct. 18, 2012), http://www.homelandsecuritynewswire.com/dr20121018-sen-rockefeller-asks-fortune-500-ceos-for-cybersecurity-best-practices.

385. Although signed on February 12, 2013, the EO was embargoed for release until after the February 13, 2013 State of the Union Address.

386. Tony Romm, *Draft Cyber Executive Order Excludes Commercial Products*, POLITICO (Nov. 30, 2012, 3:51 PM), http://www.politico.com/story/2012/11/draft-cyber-executive-order-excludes-commercial-products-84462.html#ixzz2FcFUYVZB.

387. *See* Andy Grotto, Staff Member, Senate Select Intelligence Comm., Speaking

that the Administration held off because it wanted the political cover of failed congressional legislation before issuing the EO.

When the EO was issued, it focused on two major issues: cybersecurity information sharing and the development and implementation of risk-based cybersecurity standards for critical infrastructure.[388]

1. Information Sharing

The EO's information sharing provisions build on existing DoD and DHS information sharing initiatives designed to safeguard critical defense information stored on, or transiting, the privately-owned networks of defense industrial base ("DIB") and, in some cases, CI companies. These initiatives include the DIB Cybersecurity and Information Assurance Program ("DIB CS/IA"), the DIB Exploratory Cybersecurity Initiative ("DIB Pilot"), the DIB Enhanced Cybersecurity Services ("DECS") Program, and the Enhanced Cybersecurity Services ("ECS") Program.

DoD initiated the voluntary DIB CS/IA information sharing program with DIB companies to help safeguard sensitive but unclassified DoD information on DIB unclassified networks.[389] DIB companies participating in the program are required to execute a framework agreement governing their cybersecurity information sharing with the government. Under the DIB CS/IA program, DoD provides "cyber threat information and information assurance best practices to DIB companies,"[390] and in return, DIB participants report to the government "cyber incidents that may involve DoD information" and, participate in cyberintrusion damage assessments as needed.[391] Although the program began with a limited number of DIB participants, DoD subsequently opened the program to all eligible DIB companies[392] and formalized the program through an interim

---

at ABA Section of Science and Technology Law in Washington, D.C. (Dec. 17, 2012).

388. *Compare* Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity § 1, 78 Fed. Reg. 11,737, 11,739 (Feb. 19, 2013) (discussing the policy behind the EO in section one), *with* Draft Exec. Order, *supra* note 383, § 1.

389. Memorandum from Ashton B. Carter, U.S. Deputy Sec'y of Def., on Defense Industrial Base Cyber Security 1 (Oct. 31, 2012), http://www.acq.osd.mil/dpap/policy/policyvault/OSD012537-12-RES.pdf.

390. *Id.*

391. *Id.*; Howard A. Schmidt, *Partnership Developments in Cybersecurity*, WHITE HOUSE BLOG (May 21, 2012, 2:17 PM), http://www.whitehouse.gov/blog/2012/05/21/partnership-developments-cybersecurity.

392. Dep't of Def. Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities, 77 Fed. Reg. 27,615, 27,621 (May 11, 2012) (codified at 32 C.F.R. § 236) [hereinafter DIB CS/IA Program] (setting forth DIB participant eligibility requirements); Press Release, U.S. Dep't of Def., DoD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), *available at* http://www.defense.gov/releases/release.aspx?releaseid=15266.

final rule issued May 11, 2012.[393]

The DIB CS/IA program includes an optional component known as DIB ECS ("DECS").[394] DECS specifically addresses the need to share *classified* threat information and signatures with DIB companies participating in the DIB CS/IA. Specifically, under the DECS program, the government (i.e., NSA) provides "classified cyber threat and technical information either to a DIB company or to the DIB company's Commercial Service Provider [("CSP")]."[395] DECS was based on "lessons learned" from a DoD pilot program, known as the DIB Pilot, that started back in July 2010. The DECS program ultimately became a joint DoD-DHS program "falling under the umbrella" of DHS's Enhanced Cybersecurity Services ("ECS") program[396] with DHS taking the leadership role.

The first phase of ECS "focused on the cyber protection of the DIB companies participating in DoD's [DIB CS/IA]."[397] By January 2013, DHS had decided to expand ECS to provide "enhanced cybersecurity protection" to *all U.S. CI sectors* through "the sharing of indicators of malicious cyber activity with CSPs."[398]

The success of the DIB Pilot, DECS, and ECS is unclear. While some view these programs as "an important step forward in our ability to catch up with widespread cyberthreats,"[399] others have expressed concern that "[t]he DIB pilot probably increases the defenders' work factor much more than it increases the attackers."[400] An independent review of the DIB Pilot[401] found that the program had only "marginal benefit."[402]

---

393. DIB CS/IA Program 77 Fed. Reg. 27,615.

394. DIB ENHANCED CYBERSECURITY SERVICES (DECS), http://www.dc3.mil/dcise/DIB%20Enhanced%20Cybersecurity%20Services%20Procedures.pdf.

395. Memorandum from Ashton B. Carter, *supra* note 389, at 1.

396. In January 2012, DHS and DoD announced that they would be undertaking a proof of concept known as the Joint Cybersecurity Services Pilot ("JCSP"). Under the JSCP, operational relationships with CPSs in the DIB Pilot were shifted from DoD to DHS. JCSP subsequently became known as the Enhanced Cybersecurity Services (ECS) program. *E.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE ENHANCED CYBERSECURITY SERVICE (ECS), DHS/NPPD/PIA-028 2 (2013), http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.

397. *Id.* at 2.

398. *Id.*

399. Taylor Armerding, *Will Voluntary Cyber Threat Sharing Plan Case Doubt Over CISPA?*, NETWORKWORLD (May 18, 2012, 9:20 AM), http://www.networkworld.com/news/2012/051812-will-voluntary-cyber-threat-sharing-259423.html (quoting Richard A. Hale, deputy chief information officer for cybersecurity at the NSA).

400. *Id.* (quoting Jay Healey, director of the Cyber Statecraft Initiative at Atlantic Council, a Washington, D.C. think tank).

401. *Hearing to Receive Testimony on U.S. Strategic Command and U.S. Cyber*

The EO builds on existing information sharing programs in several ways. First, the EO confirms that it is U.S. policy to improve cybersecurity information sharing, specifically by increasing the "volume, timeliness, and quality" of cyberthreat information shared with the U.S. private sector.[403] Second, the EO puts the President's imprimatur on the planned expansion of ECS to CI sectors. Specifically, the EO directs DHS and DoD to establish procedures to expand ECS to all CI sectors within 120 days.[404] Third, pursuant to the EO, unclassified versions of reports of cyberthreats to the United States that identify a specific target must be rapidly disseminated to the target.[405]

The EO also encourages the private sector to share information with the government. Toward this end, the EO provides that "[i]nformation submitted voluntarily . . . by private entities under this order shall be protected from disclosure to the fullest extent permitted by law."[406] However, private sector companies may remain reluctant to share information with the government due to the EO's lack of liability protections. The White House did not have the authority to provide liability protections through an executive order; an act of Congress is required.[407] Indeed, legislation may be necessary to address a number of

---

Command in Review of the Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program Before the S. Comm. on Armed Services, 112th Cong. 1–3 (2012) (opening statement of Carl Levin, U.S. Senator), http://www.armed-services.senate.gov/Transcripts/2012/03%20March/12-19%20-%203-27-12.pdf [hereinafter *Hearing Testimony in Review of Defense Authorization 2013*] ("Carnegie Mellon conducted an independent assessment of the DIB Pilot for DoD.").

402. Armerding, *supra* note 399 (noting that only "1% of attacks [were] . . . detected using NSA threat data that the companies did not already have themselves," according to Jay Healey, director of the Atlantic Council's Cyber Statecraft Initiative); *Hearing Testimony in Review of Defense Authorization 2013*, *supra* note 401, at 3 (opening statement of Carl Levin, U.S. Senator) ("Carnegie Mellon concluded [based on their independent assessment] that NSA provided few signatures that were not already known to the companies themselves, and in many cases, the DIB companies by themselves detected advanced threats with their own non-signature-based detection methods that probably [were] not known to the NSA."); Jason Healey, *Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More*, THE ATLANTIC (Mar. 15, 2012, 5:21 PM), http://www.theatlantic.com/technology/archive/2012/03/cybersecurity-legislation-should-force-us-government-to-listen-less-and-speak-more/254491/ ("[NSA's signature database is] considered among the crown jewels of the U.S. government's defense capabilities [but] may not be as awe-inspiring as advertised.").

403. Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity §§ 1, 4(a), 78 Fed. Reg. 11,737, 11,739 (Feb. 19, 2013).

404. *Id.* § 4(c), at 11,739–40.

405. *Id.* § 4(b), at 11,739.

406. *Id.* § 5(d), at 11,740.

407. Eric Chabrow, *Exec Order Could Ease Cybersecurity Bill Passage: Ridding Gov's Role in Setting Standards from Legislative Equation*, BANK INFO SECURITY (Dec.

issues surrounding information sharing, including the controversial privacy and civil liberties implications of such sharing.[408]

2. Cybersecurity Framework

In addition to information sharing, the EO calls for the collaborative development and voluntary adoption of a new cybersecurity framework to include risk-based cybersecurity standards for critical infrastructure.[409] The EO directs NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure ("Cybersecurity Framework");"[410] to engage in an "open public review and comment process;"[411] and to publish a final version of the Cybersecurity Framework within one year.[412] The EO directs that the Cybersecurity Framework shall include "standards, methodologies, procedures, and processes that align policy, business, and technology approaches to address cyber risk."[413] The EO requires the Cybersecurity Framework to incorporate voluntary consensus standards and industry best practices to the fullest extent possible.[414]

With an eye toward encouraging—rather than impeding—a competitive market, the EO addresses several of the concerns that industry had voiced over voluntary standards. For example, the EO clarifies that "the Cybersecurity Framework will provide [cybersecurity] guidance that is technology neutral,"[415] will not pick technological winners and losers, and will thereby "enable . . . [CI] sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks."[416]

The EO directs DHS to "establish a voluntary program to support the adoption of the Cybersecurity Framework [by CI owners and

---

7, 2012), http://www.bankinfosecurity.com/exec-order-could-ease-cybersecurity-bill-passage-a-5341.

408. *See id.* ("The more contentious matters dealing with information sharing, which also includes protecting the privacy and civil liberties of citizens whose personal information could be exposed during exchanges of data between business and government, must be addressed by legislation.").

409. Exec. Order No. 13,636 § 7(b), 78 Fed. Reg. at 11,739; Chabrow, *supra* note 407 ("At the heart of the proposed executive order is a process in which the federal government . . . would collaborate with industry to establish IT security best practices that [CI owners] . . . could adopt voluntarily.").

410. Exec. Order No. 13,636 § 7(a), 78 Fed. Reg. at 11,740–41.

411. *Id.* § 7(d), at 11,741.

412. *Id.* § 7(e), at 11,741.

413. *Id.* § 7(a), at 11,740–41.

414. *Id.*

415. *Id.* § 7(b), at 11,741.

416. *Id.*

operators]."[417] The EO explores greater use of "carrots," in the form of incentives, to promote industry participation. Indeed, it "directs the Treasury and Commerce Departments to recommend a set of possible incentives that would entice operators of critical infrastructure to join a voluntary program in which they would follow a set of cybersecurity standards."[418] The EO further directs that DHS, Treasury, and Commerce identify which incentives are available under existing law and which require legislation.[419]

The EO also seeks recommendations regarding the potential use of federal purchasing power to influence adoption of cybersecurity standards. Specifically, the EO directs DoD and the General Services Administration ("GSA"), in consultation with DHS and the Federal Acquisition Regulatory Council, to make recommendations to the President regarding the "feasibility, security benefits, and relative merits" of "incorporating security standards into acquisition planning and contract administration" as well as steps that can be taken "to harmonize . . . existing procurement requirements related to cybersecurity."[420]

In summary, the EO facilitates information sharing and the development and adoption of cybersecurity standards by CI owners and operators. Some congressional leaders fear (and some industry groups are hopeful) that the executive order sends a signal that congressional action is not urgent.[421] However, others believe that by addressing the issue of cybersecurity standards for CI owners and operators, the EO potentially removes from the legislative debate the very issue that prompted Republicans to block the compromise cybersecurity bill, and may therefore pave the way for congressional action on cybersecurity legislation in 2013.[422]

D. Congressional Action (2013)

1. U.S. House of Representatives

a. CISPA

On February 13, 2013, immediately after the EO was issued, HSPCI Chairman Rogers re-introduced CISPA.[423] CISPA passed out of committee on April 10, 2013, after a closed-door debate during which six amendments

417. *Id.* § 8(a), at 11,741.
418. *Id.*
419. *Id.*
420. *Id.* § 8(e), at 11,741.
421. *Cf.* Kelly, *supra* note 378.
422. *See* Chabrow, *supra* note 407.
423. H.R. 624, 113th Cong. (2013).

to the bill—including several amendments designed to strengthen the bill's privacy and civil liberties protections—were approved.[424] The bill's sponsors subsequently took the position that, as amended, CISPA provides appropriate protections for privacy and civil liberties.[425] Many privacy and civil liberties advocates vehemently disagreed,[426] and on April 16, 2013, just days before CISPA reached the House floor for a vote, the White House issued a veto threat, explaining that "if the bill, as currently crafted, were presented to the President, his senior advisors would recommend that he veto the bill."[427] The White House explained that "[w]hile there is bipartisan consensus on the need for . . . [cybersecurity information sharing] legislation, it should adhere to the following priorities: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections."[428] The House passed CISPA by a vote of 288-127 on April 18, 2013, just days after the Boston Marathon bombings, with Rep. Mike McCaul (R-Tex.) stating at the House hearing:

> "In the case of Boston, they were real bombs. In this case, they're digital bombs. These bombs are on their way. That's why this legislation is so urgent. For if we don't and those digital bombs land and attack the

424. Press Release, U.S. House of Representatives Permanent Select Committee on Intelligence, Bipartisan Cybersecurity Bill Clears Key Hurdle, April 10, 2013, http://intelligence.house.gov/press-release/bipartisan-cybersecurity-bill-clears-key-hurdle-0. For a textual version of the bill and its amendments, see *H.R. 624 - The Bill and Amendments*, U.S. HOUSE OF REP. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/hr-624-bill-and-amendments (last visited May 3, 2013).

425. *Myths and Facts about the Cyber Intelligence Sharing and Protection Act (CISPA)*, http://www.dutch.house.gov/CISPA%20MYTHBUSTER%202013.pdf; *see Cyber Intelligence Sharing and Protection Act of 2013*, U.S. HOUSE OF REP. PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/CivilLibertiesTPsCyberBillFeb112013v2.pdf.

426. For example, the American Civil Liberties Union decries CISPA's continued (1) lack of civilian control over domestic cyber programs; (2) failure to limit the sharing of personal information; and (3) "unlimited immunity" for hack backs. Michelle Richardson, *CISPA Remains Fatally Flawed After Secret Committee Markup*, AM. CIVIL LIBERTIES UNION (Apr. 12, 2013, 12:20 PM), http://www.aclu.org/blog/technology-and-liberty-national-security-free-speech/cispa-remains-fatally-flawed-after-secret ("We have flagged four general categories of problems in CISPA that have to be fixed before it is passed, and the markup only substantially fixed one of them . . . .").

427. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 624 – CYBER INTELLIGENCE SHARING AND PROTECTION ACT (2013), http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

428. *Id.*

United States, and Congress failed to act, then Congress has that on [its] hands."[429]

b. SECURE-IT Act

On April 10, 2013, Rep. Marsha Blackburn (R-Tenn.) re-introduced the SECURE-IT Act in the House.[430]

2. U.S. Senate

On the Senate side, Senators Tom Carper, John D. Rockefeller IV, and Diane Feinstein introduced the Cybersecurity and American Cyber Competitiveness Act of 2013[431] on January 23, 2013. Despite its impressive title, the legislation is nothing more than a "sense of Congress" that there *should* be legislation.[432] In his press release announcing the bill, Senator Carper stated: "It is a priority this year to act on comprehensive cybersecurity legislation."[433]

Senator Feinstein has since announced her intention to introduce information sharing legislation through the Senate Intelligence Committee, which she chairs.[434]

E. Regulatory Litigation

Recent regulatory litigation developments, such as *Federal Trade Commission ("FTC") v. Wyndham*, should inform corporate cybersecurity investments.[435] *Wyndham* marks the first time that the FTC has sued a major company in federal court for failure to *secure* customer information. The FTC's suit alleges that Wyndham and its subsidiaries had flawed security practices (including failure to erect firewalls, use appropriate

429. Elizabeth Flock, *Texas Congressman Uses Boston Bombing to Argue for CISPA Passage*, U.S. NEWS & WORLD REPORT (Apr. 18, 2013), http://www.usnews.com/news/blogs/washington-whispers/2013/04/18/texas-congressman-uses-boston-bombing-to-argue-for-cispa-passage.

430. H.R. 1468, 113th Cong. (2013).

431. S. 21, 113th Cong. (2013).

432. *Id.* § 3.

433. Press Release, Tom Carper, U.S. Senator, Comprehensive Cybersecurity Bill Will Be Priority this Congress (Jan. 23, 2013), *available at* http://www.carper.senate.gov/public/index.cfm/pressreleases?ID=99646255-b703-4647-96e5-c1c4e9fdc1a4.

434. Katy O'Donnell, *Intelligence Leaders: Cybersecurity Now the Top Global Threat*, MAIN JUST. (March 13, 2013, 9:38 AM), http://www.mainjustice.com/2013/03/13/intelligence-leaders-cybersecurity-now-the-top-global-threat/ (quoting Senator Feinstein saying that she and Senator Chambliss will begin an effort shortly to "see if we can't get a bill that we can agree to move through the [Senate Intelligence] committee on the information-sharing part of it.").

435. Complaint, FTC v. Wyndham Worldwide Corp., filed (D. Ariz. 2012) (No. 2:12-cv-01365-SPL), http://ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf.

passwords, or configure software to keep credit card information secure).[436] FTC officials have called the alleged security flaws "obvious."[437]

In the *Wyndham* complaint, the FTC claims that Wyndham's security practices constitute both unfair and deceptive practices in violation of the FTC Act. First, the FTC alleges that Wyndham's failure to safeguard personal information caused substantial consumer injury and constituted an unfair practice. Second, the FTC alleges that Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information.[438] The FTC alleges, for example, that Wyndham failed to keep up with industry cybersecurity standards despite promising to do so in its own privacy policy.[439]

In *Wyndham*, the FTC essentially is asserting that it can use its enforcement authority to hold companies to their data security promises, including promises to adopt "reasonable security measures." As the FTC litigates more of these cases, a body of legal rulings is likely to develop regarding the meaning of "reasonable security."[440] Such rulings potentially could eventually serve as a basis for tort liability (i.e., liability for failure to take reasonable security measures), which likely explains why the U.S. Chamber of Commerce, through the National Chamber Litigation Center, has filed an amicus brief on behalf of the defendants in *Wyndham*, urging the Court to grant Wyndham's motion to dismiss.[441]

Wyndham also serves as a cautionary tale, reminding corporations of the care that must be taken when drafting corporate data security policies governing the handling of consumer information. It is imperative that corporations ensure that their data security policies accurately describe their data security practices and make only those promises that the

436. *See id.* at 10.

437. Craig Timberg, *FTC Sues Wyndham Hotels over Hacker Breaches,* WASH. POST (June 26, 2012), http://articles.washingtonpost.com/2012-06-26/business/35459761_1_hackers-personal-data-information-security.

438. Complaint at 17, *Wyndham Worldwide Corp.*, (No. 2:12-cv-01365-SPL).

439. *Id.* at 18–19.

440. In a recent non-regulatory litigation that may signal the "future of business-to-business litigation," according to Crowell & Moring LLP partner David Bodenheimer, an Oregon company reportedly sued its bank to recover nearly a quarter of a million dollars that cyberthieves stole from its accounts. The company reportedly alleged that the bank violated the requirements for commercially reasonably security procedures set forth in Uniform Commercial Code Section 4A. Brian Krebbs, *Hay Maker Seeks Cyber Heist Bale Out*, KREBS ON SECURITY, April 13, 2013, http://krebsonsecurity.com/2013/04/hay-maker-seeks-cyberheist-bale-out/; *see* Complaint at 1, Oregon Hay Prod., Inc. v. Cmty. Bank (Or. Cir. Ct.) (No. CVH120083).

441. *See* Brief for U.S. Chamber of Commerce et al. as Amici Curiae Supporting Defendants, FTC v. Wyndham Worldwide Corp., filed (D. Ariz. 2012) (No. 12-1365-SPL).

corporation can and will keep.

VI. PRIVATE SECTOR CHALLENGES

The basic problem—true since 1998—is there are no incentives sufficient to make companies in most critical infrastructure sectors take voluntary action to bring the security of their networks to the level needed for national defense.
- James A. Lewis, CSIS[442]

A. The Limits of Vulnerability Mitigation

The U.S. self-regulatory approach to ".com" cybersecurity has long been heavily focused on vulnerability mitigation. Behind the fancy language is a simple idea: that by strengthening our cyberdefenses we will better protect the ".com" domain against cyberthreats, including cybercrime, cyberespionage, and cyberwar. Yet, by all accounts, it appears that we remain quite vulnerable to cyberthreats.

Many experts believe that our continued vulnerability stems from chronic private sector underinvestment in cyberdefenses, particularly with respect to critical infrastructure.[443] Some companies simply fail to make investments in even the basic vulnerability mitigation measures necessary to protect against the cyberthreats posed by "script-kiddies" and run-of-the-mill cybercriminals.[444] Other companies may invest in cyberdefense to protect their own assets, but their investments rarely reflect the fact that, as the nation becomes increasingly interconnected, one company's vulnerabilities may result in harm to another company—or even the nation. As cybercrime, cyberespionage, and cyberwar proliferate, the consequences of inadequate cyberdefenses will only mount.

More fundamentally, in some contexts, our nation's focus on vulnerability mitigation may be misplaced. While good cyberdefenses may be sufficient to ward off certain cyberthreats (e.g., opportunistic cybercrimals), they likely will be insufficient to keep determined adversaries, such as nation-state actors, from perpetrating cyberespionage or cyberwar. This problem will only be exacerbated as malware "trickles down"[445] from nation-state actors to cybercriminals,[446] and as hacking tools

442. Lewis, *supra* note 308.

443. *See* Letter from Michael Chertoff et al. to Harry Reid & Mitch McConnell, *supra* note 182.

444. Panetta, Remarks on Cybersecurity, *supra* note 223 ("[T]he reality is that too few companies have invested in even basic cybersecurity.").

445. Robert Bigman, *Guest Blog: Former CIA CISO on Nation-State Security Challenges*, FIREEYE BLOG (June 15, 2012), http://blog.fireeye.com/research/2012/06/former-cia-ciso-national-security.html ("[A]dditional attacks (mostly kernal rootkits) have appeared that reflect the 'trickle down' of APT technology from nation-states to

are commoditized.

Accordingly, it may be worthwhile to view vulnerability mitigation as but one part of a more holistic ".com" cybersecurity strategy that seeks not only to defend cyberspace, but also to deter threat actors. Today, nation-states and nation-state sponsored actors engaged in cyberespionage face few, if any, consequences for their actions. The U.S. private sector could play an important role in shifting the focus of cybersecurity efforts toward threat deterrence, potentially through its own actions, and also by encouraging the U.S. government to explore ways to bring all elements of national power—including economic, diplomatic,[447] and military—to bear on the evolving cyberthreat.

B. Obstacles to Effective Vulnerability Mitigation

According to experts, one of the key challenges to vulnerability mitigation is the difficulty of spurring adequate private sector investment in cyberdefense, a difficulty that may stem from a variety of sources, including the widely-acknowledged lack of reliable cyberincident data;[448] the "it can't happen to me" mentality evidenced by some corporations; and the "public good" nature of cybersecurity.

---

the cybercriminal industry . . . . [T]he Chinese government engaged cybercriminals to assist in the development and peer review of the Aurora attack code and even shared the final product with them.").

446. Matthew J. Schwartz, *7 MiniFlame Facts: How Much Espionage Malware Lurks?*, INFORMATIONWEEK (Oct. 17, 2012, 12:56 PM), http://www.informationweek.com/security/management/7-miniflame-facts-how-much-espionage-mal/240009237 ("Another worry from nation states' malware espionage operations is that their tricks will soon be put to use by criminals. In a 2009 report on malware used for surveillance purposes, Cambridge University researchers Shishir Nagaraja and Ross Anderson wrote, 'What Chinese spooks did in 2008, Russian crooks will do in 2010 and even low-budget criminals from less developed countries will follow in due course.' In other words, how long will it be until today's Flame [cyberattack malware] becomes the inspiration for tomorrow's financial malware attack?").

447. *See, e.g.*, Press Release, Kirsten Gillibrand, U.S. Senator Gillibrand Announces New Cybersecurity Bill Includes Measures She Authored to Combat Global Cyber Criminals (Feb. 15, 2012), *available at* http://www.gillibrand.senate.gov/newsroom/press/release/gillibrand-announces-new-cybersecurity-bill-includes-measures-she-authored-to-combat-global-cyber-criminals ("[The new bill] authorize[es] a State Department official to coordinate U.S. diplomatic strategy to combat cybercrime and establish a consistent foreign policy when it comes to cybercrime issues across relevant federal departments, agencies, U.S. embassies, and consulates.").

448. Deirdre K. Mulligan & Fred B. Schneider, *Doctrine for Cybersecurity*, DAEDALUS, Fall 2011, at 70, 73, http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf ("[The] lack of information about vulnerabilities, incidents, and attendant losses makes actual risk calculations difficult.").

1. Lack of Cyberincident Data Necessary to Calculate ROI

Executives understandably may be reluctant to invest in cybersecurity without a clear understanding of the return on investment ("ROI")[449] for their cybersecurity dollar because cybersecurity is expensive and can easily become a "black hole"[450] for spending. Unfortunately, the industry lacks reliable ROI data upon which to build a business case for increased cyber defense investments.

Reliable ROI data depends on reliable data about the frequency of cyberincidents, the costs of cyberincidents, and the effectiveness of mitigation methods. Reliable cyberincident information is lacking, both because corporations may be victimized without their knowledge,[451] and because corporations may be reluctant to report cybersecurity breaches,[452] for fear of repercussions in terms of compromised cybersecurity, competitiveness, regulatory risk, consumer response, cost, and/or reputation.[453] Without reliable data about the frequency of cyberincidents, it is difficult for companies to calculate the probability with which

449. *See* Simon Moffatt, *Information Security: Why Bother?*, INFOSEC ISLAND (Dec. 9, 2012), http://www.infosecisland.com/blogview/22774-Information-Security-Why-Bother.html ("Organisations have finite budgets which will cover all of IT and related services, and it is a fair objective, to have to show and prove, either via tangible or intangible RoI, that a piece of software or consultancy will have a beneficial impact on the organisation as a whole.").

450. Erik Sherman, *Hackers Target Small Businesses*, CBS NEWS: MONEYWATCH (July 6, 2012, 11:05 AM), http://www.cbsnews.com/8301-505124_162-57467265/hackers-target-small-businesses/.

451. ALPEROVITCH, *supra* note 96, at 2 ("I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact."); Kellermann, *supra* note 142 ("55% of our customers had to be *informed* that they had a breach versus actually being aware themselves.") (emphasis added); Perlroth, *supra* note 111 (experts say the majority of cyberattacks go "undisclosed or unnoticed"); Andrea Shalal-Esa, *Scores of U.S. Firms Keep Quiet About Cyber Attacks*, REUTERS (June 13, 2012, 3:08 PM), http://www.reuters.com/article/2012/06/13/net-us-media-tech-summit-cyber-disclosur-idUSBRE85C1E320120613 (" '[M]any corporations were unaware that their networks had been breached until FBI agents notified them that they discovered proprietary, company-specific data outside their networks,' [according to Shawn Henry, the FBI's 'former top cyber cop.'] ").

452. Shalal-Esa, *supra* note 451 (" 'There have been lots of breaches in every industry that have never been publicized,' said Shawn Henry . . . .").

453. *See* Gorman & Tibken, *supra* note 162 (" 'It would have been better if RSA was more forthright from the beginning [of their breach]. They unnecessarily damaged their reputation by holding back,' said [one] Gartner analyst . . . . [RSA CEO Art Coviello] said his company has provided the right amount of information to its customers. Providing any further information, he said, would give the hackers a blueprint for how to mount further attacks."); *CF Disclosure Guidance*, *supra* note 288 (discussing concerns that detailed corporate cyberincident disclosures could provide a "roadmap" for adversaries seeking to compromise corporate network security).

cyberincidents are likely to strike. Similarly, reliable information about both the tangible and intangible costs associated with cyberincidents is lacking, not only because corporations are reluctant to report cyberincidents, but also because of the practical difficulty of measuring certain costs, including opportunity costs and the costs associated with reputational harm, loss of consumer confidence, intellectual property loss, and loss of consumer privacy.[454] Finally, the effectiveness of mitigation methods is unknown.

Despite the importance of reliable cyberincident data, a recent survey of 1000 publicly-traded companies revealed that "[fifty-two] percent failed to report . . . network breaches."[455] Experts believe that many corporations fail to report cyberincidents, despite reporting obligations under data breach notification laws and other applicable disclosure rules, such as the SEC's cybersecurity guidance. One cybersecurity expert points to the telling example of a publicly traded defense contractor whose IP was exfiltrated to China as a result of a cyberintrusion. The company decided not to disclose the intrusion and, as justification for its decision, stated that the company "only do[es] business with the U.S. government and it doesn't really matter that the Chinese stole all their IP because the U.S. government will never buy from China, so it wasn't really material to them."[456] So long as companies continue to withhold cyberincident data, obtaining reliable calculations of ROI for cyberdefense spending will remain problematic.

2. "It Can't Happen to Me" Mentality

Whether due to lack of cyberincident data or otherwise, some companies view themselves as immune from cyberthreats. Consider the case of small- and medium-sized businesses ("SMBs"). SMBs are attractive cyber targets because they traditionally have weaker cyberdefenses than larger businesses due to resource constraints.[457] Attacks on SMBs recently accelerated, with the number of targeted attacks against SMBs doubling in the last half of 2012.[458] Moreover, companies with 100 or fewer employees

454. *See generally* ANDERSON ET AL., *supra* note 139 (discussing the difficulties of precisely measuring indirect losses from cybercrime, such as loss of consumer confidence). Estimating cyberespionage costs is also difficult as "there is no reliable data available." *See id.* (criticizing a UK report in which "the authors admit the proportion of IP actually stolen cannot currently . . . be measured with any degree of confidence, so they assign probabilities of loss and multiply by sectoral GDP").

455. Shalal-Esa, *supra* note 451 (citing 2011 SAIC study).

456. *See id.*

457. *See* Sherman, *supra* note 450 (describing SMBs as "perfect prey" because they "tend to lack the resources to fully secure their computer systems," yet they also tend to have "significant amounts of money").

458. Andy Singer, *SMBs—the Weakest Link in the Cybercriminal Supply Chain?*, SYMANTEC (July 10, 2012), http://www.symantec.com/connect/blogs/smbs-weakest-

were the victims in sixty-three percent of data breaches Verizon analyzed in a 2010 study.[459]

Despite their vulnerability, some SMBs have failed to take even the most basic corporate security steps. For example, nearly ninety percent of SMBs have no formal internet security policy and nearly seventy percent lack even an informal policy, according to a recent survey jointly conducted by the National Cyber Security Alliance ("NCSA") and global security solutions provider Symantec.[460] Nearly sixty percent of SMBs do not even have a backup plan in case of a data breach, notwithstanding the significant costs associated with such breaches.[461]

On the whole, the SMBs surveyed by NCSA/Symantec are surprisingly unconcerned about cybersecurity. According to the survey: (1) over eighty percent of SMBs are satisfied with the amount of data security they provide and think they are investing adequate resources in cybersecurity;[462] (2) seventy-seven percent said that their companies are safe from cyberthreats including hackers, breaches, viruses, and malware;[463] and (3) sixty-six percent of SMBs are not concerned about an external or internal cybersecurity threat.[464] Moreover, seventy percent said they have no employee social media usage policy despite the fact that social media can leave businesses more vulnerable to phishing and other social-engineering

---

link-cybercriminal-supply-chain ("[T]here appears to be a direct correlation between a rise in attacks against small companies and a drop in attacks against larger ones, which could mean that attackers are diverting resources directly from one group to the other. Even though larger businesses (2500+ employees) continue to be the primary target for most targeted attacks . . . the gap between the two is quickly closing.").

459. Sherman, *supra* note 450.

460. Press Release, Symantec, New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have no Policies or Contingency Plans (Oct. 15, 2012), *available at* http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01.

461. *Id.*; *Ponemon Study Shows the Cost of a Data Breach Continues to Increase*, PONEMON (Jan. 25, 2012), http://www.ponemon.org/news-2/23 (noting that in a study of forty-five data breach cases, the most expensive data breach cost the affected company $31 million to resolve; the least expensive cost $750,000, emphasizing that most of the costs are from legal defense spending).

462. NAT'L CYBERSECURITY ALLIANCE & SYMANTEC, 2012 NATIONAL SMALL BUSINESS STUDY (2012) http://www.staysafeonline.org/download/datasets/4393/2012_ncsa_symantec_small_business_study_fact_sheet.pdf.

463. *Id.*; *Small Business Online Security Infographic*, STAYSAFEONLINE.ORG, http://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic (last visited Apr. 2, 2013).

464. Scott Cornell, *SMBs in the U.S. Are Soft on Cybersecurity*, FARONICS (Nov. 6, 2012), http://www.faronics.com/2012/smbs-in-the-u-s-are-soft-on-cybersecurity/; Press Release, Symantec, *supra* note 460 ("Visa Inc. reports that small businesses represent more than 90 percent of the payment data breaches reported to the company.").

based cyberincidents.[465]

This "it can't happen to me" mentality has the potential to lead to particularly grave consequences in the current environment, where bad actors are increasingly setting their sights on corporations "low down in the security supply chain as a stepping-stone, with the expectation that they will have less robust security features in place than the top-tier defense contractors or government agencies they ultimately want to target."[466] Today's environment necessitates greater awareness of cyberthreats among SMBs, as well as the companies they supply.

3. "No Corporation Is An Island": Cybersecurity as a Public Good

According to many experts, another key challenge to achieving optimal (or even adequate) private sector investment in cyberdefenses is the fact that cybersecurity is a public good.[467] One company's underinvestment in cyberdefense can redound to the detriment of other companies with whom they connect. Indeed, "a single compromised system anywhere in a network can serve as a launching point for attack on other systems connected to that network."[468] Some companies—e.g., SMBs—may be motivated to invest sufficiently to protect their own assets, but are unlikely to invest sufficiently to protect the assets of companies with whom they do business, leading some experts to conclude that "the private sector will not supply adequate cybersecurity on its own; it's a public good that's missing as the result of market failure."[469] As our interconnectedness grows, the problem is only exacerbated.

---

465. NAT'L CYBERSECURITY ALLIANCE & SYMANTEC, *supra* note 462; *Small Business Online Security Infographic*, *supra* note 463.

466. Ben Weitzenkorn, *'Aurora' Google Hackers Still an Active Threat, Report Says*, TECHNEWSDAILY, (Sept. 10, 2012, 2:37 PM), http://www.technewsdaily.com/8090-aurora-google-hackers-active-threat.html; *see* Singer, *supra* note 458 ("[W]hile your business may not be the primary target of an attack, cybercriminals may be using your organization as a stepping-stone to attack other businesses . . . SMBs typically don't have the resources to maintain a full IT staff, so [they] could be seen as a weaker link in the supply chain.").

467. Mulligan & Schneider, *supra* note 448, at 75 ("Cybersecurity is non-rivalrous and non-excludable; by definition, it is a *public good.* It is non-rivalrous because one user benefiting from the security of a networked system does not diminish the ability of any other user to benefit from the security of that system. And it is non-excludable because users of a secure system cannot be easily excluded from benefits security brings.") (emphasis in original); *see* Bruce H. Kobayashi, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goals* 5 (Geo. Mason Univ. Sch. of L., Working Paper Series, Paper 26, 2005), *available at* http://law.bepress.com/gmulwps/gmule/art26.

468. Mulligan & Schneider, *supra* note 448, at 74.

469. David Perera, *Lewis: Common Assumptions About Cybersecurity Are Wrong*, FIERCEGOVERNMENTIT (Sept. 28, 2011), http://www.fiercegovernmentit.com/story/lewis-common-assumptions-about-cybersecurity-policy-are-wrong/2011-09-28.

Moreover, when companies calculate their optimal level of investment in cybersecurity, they consider their own risks (e.g., risk of IP loss from an intrusion and the cost of such loss), but not the broader set of potential risks, including not only risks to other companies with whom they are connected, but the potential societal risks to our nation's economic or national security from successful cyberespionage or cyberattack. Companies invest in cybersecurity to protect their own assets from cyberthreats, but their investments are unlikely to account for the potential harm to our economic or national security in the event of a cyberincident. Specifically, "[c]ompanies assess the probability that a threat will become an attack, and if there is an attack, whether they will be held liable. They weigh the cost of preventive measures against the risk of liability. Almost all conclude that the liability risk for cyberattack is too low to justify greater effort. This is a sensible business decision but does not help national security."[470]

C. *Failure of Vulnerability Mitigation in the Face of Determined Adversaries*

While there are many challenges to effectively mitigating vulnerabilities, more fundamentally, our nation's focus on cybersecurity through vulnerability mitigation may be misplaced. It has become apparent from the trajectory of both cybercrime and cyberespionage losses that even sophisticated corporate vulnerability mitigation efforts do not thwart the most concerted adversaries (e.g., nation-state adversaries, terrorists, sophisticated cybercriminals, and hacktivists). Even organizations with highly sophisticated cybersecurity programs (e.g., DoD, RSA Security, Lockheed Martin, and Google) are not immune from successful penetration by determined adversaries.

Vulnerability mitigation may be failing against determined adversaries because, when it comes to sophisticated cybersecurity, the offense (i.e., threat actor) currently has a substantial advantage over the defense (i.e., cyberdefender).[471] Offense is cheaper, more agile,[472] better organized,[473]

470. Lewis, *supra* note 308.

471. Some simple examples demonstrate this point. First, it only takes "a couple hundred lines of code to . . . sneak . . . something out of somebody's network," but it can take "at least a million lines of code to patch [the vulnerability]" and there is "more area to attack with every patch. . . . Everything is in the favor of the attacker." James E. Cartwright, General (Retired), Address at the Center for Strategic and International Studies, Global Security Forum 2012: Fighting a Cyber War (Apr. 11, 2012), http://csis.org/files/attachments/120411_FightingACyberWar_GSF_Transcript.pdf. Moreover, if there are twenty vulnerabilities in a networked information system, the offense needs to exploit only one to be successful while the defense may need to find and patch all twenty to successfully keep out a determined adversary. *See, e.g.*, King, *supra* note 141 ("The defenders have to be good everywhere; the attacker only has to

has no boundaries,[474] and has no legal obstacles with which to contend.[475] When confronted with sophisticated cyberdefenses, determined adversaries can redouble their efforts to exploit and target vulnerabilities or circumvent the target's cyberdefenses altogether using relatively unsophisticated social engineering-based attacks, such as those used to successfully penetrate RSA Security.[476] Additional defensive measures may bring no additional protection in real terms (i.e., companies still may be vulnerable), so it is not surprising to learn that companies weighing the cost of additional cybersecurity measures against the costs of not taking such measures frequently decide not to act.

For all of these reasons, corporate executives are understandably skeptical regarding the return on investment from dollars spent on vulnerability mitigation and have difficulty seeing the business case for increased cybersecurity resource expenditures. Section VII discusses a number of ways in which corporations can begin successfully to address the daunting cybersecurity challenges they face.

VII. PRIVATE SECTOR OPPORTUNITIES

A. Pathways to Effective Vulnerability Mitigation

As the U.S. private sector strives to bolster cybersecurity, due consideration should be given to: (1) basic cyberhygiene to protect against opportunistic cyberintrusions; (2) improved situational awareness through

---

be good on one place."). Consider the challenges involved in successfully securing a complex and interconnected system such as the smartgrid—our nation's next generation electric grid—or the current electric grid, where security has been "bolted on" because it was not originally "designed in." *Cf.* MITRE CORP., STANDARDIZING CYBER THREAT INTELLIGENCE INFORMATION WITH THE STRUCTURED THREAT INFORMATION EXPRESSION (STIX™) 3 (2012), http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf (considering how "intelligence-driven" computer network defense could potentially challenge the "conventional wisdom" that offense has an inherent advantage over defense and discussing potential opportunities to "fundamentally affect the balance of power between the defender and the adversary").

472. The cyberthreat against which companies are defending is constantly evolving with the result that "[e]ven big companies with significant IT staffs have difficulty keeping up with all the changes, updates, modifications, and upgrades necessary to keep up with the world of criminal hacking." Sherman, *supra* note 450.

473. SANS INST., AN UNEVEN PLAYING FIELD: THE ADVANTAGES OF THE CYBER CRIMINAL VS. LAW ENFORCEMENT—AND SOME PRACTICAL SUGGESTIONS 3–5 (2002), http://www.sans.org/reading_room/whitepapers/legal/uneven-playing-field-advantages-cyber-criminal-vs-law-enforcement-and-practica_115.

474. *Id.* at 7.

475. *Id.*

476. Bright, *supra* note 86 (calling the attack on RSA "run-of-the-mill" and explaining that it was not "extremely sophisticated" as originally suggested by RSA).

threat intelligence; and (3) adoption of cyberinsurance to manage the consequences of inevitable cyberintrusions.

1. Cyberhygiene

Many cybersecurity experts believe that basic cyberhygiene is a simple and logical first step in corporate cybersecurity.[477] Estimates suggest that good cyberhygiene could prevent up to eighty-five percent of cyber-intrusions, according to Howard Schmidt, former cybersecurity coordinator for President Obama.[478] Rather than waiting for legislative mandates or a cyberincident to spur corporate cybersecurity spending, corporations would be wise to consider whether some proactive investments in basic cyber-hygiene[479] are warranted as part of their basic corporate responsibility.[480] However, some argue that even basic cyberhygiene is expensive, if not cost-prohibitive, for some companies. A recent study lends some credence to that claim. Based on interviews with technology managers from 172 U.S. organizations in six industries, the study found that "[t]o be able to thwart 84 percent of attacks, up from the current 69 percent, respondents said they would have to almost double their average expenditures on

477. *A Brief History of the 20 Critical Security Controls*, SANS INST., http://www.sans.org/critical-security-controls/history.php (last visited Apr. 2, 2013) ("[T]he Commander of the US Cyber Command and Director of NSA announced that he believed adoption of the 20 Critical Controls was a good foundation for effective cybersecurity.").

478. *See* Howard Schmidt, *Price of Inaction Will Be Onerous*, N.Y. TIMES (Oct. 18, 2012), http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest ("It is estimated that as high as 85% of successful intrusions could have been prevented by just implementing good 'cyber-hygiene.' "); *see also* Press Release, Mac Thornberry, U.S. Representative, Cybersecurity Task Force Releases Recommendations (Oct. 5, 2011), *available at* http://thornberry.house.gov/news/documentsingle.aspx ?DocumentID=263044 ("The consensus among experts is that 85% of current cyberthreats can be thwarted by current cyber hygiene."). According to the Australian Department of Defence, "[a]t least 85% of the targeted [cyberintrusions] that the Defence Signals Directorate (DSD) responded to in 2010 could have been prevented by following the first four mitigation strategies listed in DSD's Top 35 Mitigation Strategies." *Strategies to Mitigate Targeted Cyber Intrusions*, AUSTRALIA DEP'T OF DEF.—DEF. SIGNALS DIRECTORATE, http://www.dsd.gov.au/infosec /top35mitigationstrategies.htm (last visited Apr. 2, 2013) (describing the top four mitigation strategies as: patching applications, such as Java and Microsoft Office; patching operating system vulnerabilities; minimizing the number of users of with administrative privileges; and application "whitelisting" which allows users to run only approved applications).

479. *See* John Brennan, *Cybersecurity Awareness Month Part III*, WHITE HOUSE BLOG (Oct. 19, 2009, 4:39 PM), http://www.whitehouse.gov/blog/Cybersecurity-Awareness-Month-Part-III (providing "tips" for improved cyber hygiene).

480. Ann Goodman, *Digital Security: Business's Social Responsibility*, ANN GOODMAN'S BLOG (July 1, 2012), http://anngoodman.com/2012/07/01/digital-security-a-business-social-responsibility/.

equipment and practices such as user verification systems, encryption and workforce training."[481]

2. Situational Awareness Through Threat Intelligence

Improving our nation's cybersecurity requires companies not just to invest *more* in cybersecurity, but to invest *wisely*. Today, many companies invest their cybersecurity dollars in intrusion detection systems and other perimeter defense systems designed to detect breaches. Cybersecurity experts have begun to challenge the "breach prevention" model of cybersecurity. For example, one expert writes:

> [W]e stubbornly adhere to Einstein's definition of insanity: doing the same thing over and over again and expecting a different outcome. In this case, that same thing is responding to breaches by investing disproportionate sums of money in perimeter defenses in a futile attempt to prevent breaches.
>
> . . . .
>
> Stop pretending you can prevent a perimeter breach. Accept that it will happen and build your security strategy accordingly. We need to admit that we, as an industry, have a problem. Start by asking yourself if your security philosophy has changed much in the last 10 years. It almost certainly has not. You're likely to be spending 90% of your security budget the same way you did back in 2002, which undoubtedly focuses on perimeter and network defenses.[482]

Perimeter defense systems do not tell you who is on your system, so once an adversary penetrates the network without being detected,[483] he may lurk undetected for years, as was the case with Operation Shady RAT.[484] Better situational awareness of corporate networks through threat intelligence is just one example of the ways in which corporations

---

481. Eric Engleman & Chris Strohm, *Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps*, BLOOMBERG (Jan. 31, 2012, 12:00 AM), http://www.bloomberg.com/news/2012-01-31/cybersecurity-disaster-seen-in-u-s-survey-citing-spending-gaps.html.

482. Tsion Gonen, *Breach Prevention is Dead. Long Live the 'Secure Breach,'* NETWORK WORLD (Oct. 29, 2012, 5:21 PM), http://www.networkworld.com/news/tech/2012/102912-secure-breach-263779.html.

483. Joseph Menn, *Hacked Firms Fight Back with Vigilante Justice*, GLOBE & MAIL (June 18, 2012, 1:58 PM), http://www.theglobeandmail.com/technology/tech-news/hacked-firms-fight-back-with-vigilante-justice/article4321501/ ("Consumer-grade antivirus you buy from the store does not work too well trying to detect stuff created by the nation-states with nation-state budgets.").

484. *See generally* ALPEROVITCH, *supra* note 96; Larry Greenemeier, *No Hacktivism Here: McAfee Reveals Cyber Espionage That Went Undetected for Years*, SCI. AM. (Aug. 3, 2011), http://blogs.scientificamerican.com/observations/2011/08/03/no-hactivism-here-mcafee-reveals-cyber-espionage-that-went-undetected-for-years/.

vulnerable to cyberespionage threats may be able to ramp up their cyberprotections.

For companies handling sensitive customer information, encryption is another relatively simple security measure to be considered.[485] Online retailer Zappos recently suffered a breach in which the attacker accessed customer information, but it is believed that the attackers received "virtually nothing of value from the theft" because the data was encrypted.[486] Some have even noted that the intrusion could "well make Zappos more secure moving forward, since potential attackers will know the company represents a poor investment of their time and effort."[487]

3. Insurance

Cybersecurity is much more than just a technical challenge. Recognizing that perfect security generally is unattainable, unnecessary, and cost-prohibitive,[488] most companies embrace risk management (i.e., managing the risk of loss due to cyberincidents) as a central element of information security.[489] The motivating principle behind the risk management approach to cybersecurity is to invest in security so as to reduce "expected losses" from attacks.[490] Such losses may include

485. Effective encryption implementations require, *inter alia*, successful key management and robust access controls. *See* VORMETRIC, DATA PROTECTION FOR PHYSICAL, VIRTUAL, AND CLOUD ENVIRONMENTS 1–2 (2012), http://www.vormetric.com/sites/default/files/sb-physical-virtual-cloud-environments-data-protection.pdf.

486. Gonen, *supra* note 482.

487. *Id.*

488. Kenneth L. Wainstein & Keith M. Gerver, *The Rockefeller Letter and the Cybersecurity Debate*, LEXOLOGY (Oct. 12, 2012), http://www.lexology.com/library/detail.aspx?g=a50ee1c0-2931-4550-9aaf-cc8da1dfe7c0 ("[O]ne recent survey of 172 U.S. companies found that they would have to boost their cyber spending almost 900% to achieve a level of security that would stop 95% of cyberattacks."); Engleman & Strohm, *supra* note 481 ("To achieve an ideal level of security in which 95 percent of attacks are thwarted, utilities and energy companies surveyed in the Bloomberg study would have to increase average annual spending more than seven-fold to $344.6 million per company from the current level of $45.8 million.").

489. In fact, critical infrastructure companies participating in a recent Bloomberg study said that they would need to nearly double their cybersecurity spending to improve the security of their systems, and even then would "remain vulnerable." Helen Domenici & Afzal Bari, *BGOV Study: The Price of Cybersecurity: Big Investments, Small Improvements*, BLOOMBERG GOV'T BLOG (Feb. 1, 2012), http://about.bgov.com/2012/02/01/bgov-study-the-price-of-cybersecurity-big-investments-small-improvements/; *see* ALPEROVITCH, *supra* note 96, at 6 (discussing how the availability of countermeasures against the bad actor "caused the perpetrator to adapt and increasingly employ a new set of implant families and [Command & Control] infrastructure").

490. Mulligan & Schneider, *supra* note 448, at 6.

reputational risk;[491] potential loss of valuable intellectual property; regulatory risk (e.g., regulatory penalties imposed for cybersecurity failure or failure to satisfy data breach notification requirements); and liability for loss due to negligence (e.g., liability for harm to consumers arising out of penetration of inadequately secured corporate networks).

Cyberinsurance is an important private sector risk-management tool. Over the past decade, the insurance industry's response to cyberrisks has evolved significantly. Initially, many standard policies were worded broadly enough to cover losses arising out of cybersecurity breaches; however, insurance companies quickly recognized this and moved to exclude cyberrisks from their standard coverage. To fill the resulting gap in coverage, insurers began marketing specialized cyberinsurance policies.[492]

Cyberinsurance has a number of important benefits. Specifically,

> Cyber-insurance increases cyber-security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security. The security requirements used by cyber-insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber-losses, they have a strong interest in greater security, and their requirements are continually increasing. [493]

Accordingly, a well-functioning cyberinsurance market could help to "align private incentives with the overall public good."[494]

Despite the potential benefits of cyberinsurance, the industry has been slow to purchase policies, with only about thirty-five percent of public companies currently investing in such coverage.[495] In some cases,

---

491. Gorman & Tibken, *supra* note 162 (noting that despite mitigation measures, a security breach will still hurt RSA's reputation).

492. Louis Chiafullo & Brett Kahn, *Coverage for Cyber Risks*, COVERAGE, ABA SECTION ON LITIG., COMMITTEE ON INS. COVERAGE LITIG., May/June 2011, at 3, 7, http://www.meagher.com/files/upload /Coverage_MayJune2011_Woodworth.pdf.

493. WHITE HOUSE, CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY 1–2, http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

494. Walter S. Baer & Andrew Parkinson, *Cyberinsurance in IT Security Management*, IEEE SECURITY & PRIVACY 50 (2007), http://www.sis.pitt.edu /~dtipper/2825/CIn.pdf.

495. *See Chubb 2012 Public Company Risk Survey: Cyber—Did You Know?*,

executives may not think that their companies are vulnerable to attack, and, in other cases, cyberinsurance simply may be cost-prohibitive.[496]

2013 may be the year of cyberinsurance as executives (1) come to better understand the threats of cybercrime, cyberespionage, and cyberwar; and (2) deal with legal and regulatory developments, including the SEC's game-changing cybersecurity guidance issued in October of 2011.[497] This staff-level guidance not only clarifies that companies must report "material information regarding cybersecurity risks and cyber incidents," but also provides that "to the extent material, appropriate disclosures may include . . . [d]escription of relevant insurance coverage."[498] The SEC's staff guidance is expected to spur corporate interest in cyberinsurance,[499] as would the more formal SEC guidance Senator Rockefeller has urged the SEC to adopt.[500]

Some foresee a system in which (1) civil liability is imposed for cybersecurity breaches (possibly with safe harbors or other limitations on

---

CHUBB GRP. OF INS. COS., http://www.chubb.com/infographics/chubb3/index.html (last visited Apr. 2, 2013); *see also* Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. TIMES BITS BLOG (Dec. 29, 2011, 10:50 AM), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/ ("[O]nly a third of companies surveyed by Advisen, a research group, say they have purchased a cyber insurance policy.").

496. Specialized cybercoverage is expensive for a number of reasons. First, considerable uncertainty remains about the appropriate pricing of cyberinsurance policies. While insurers are aware of the risk of very large losses, they lack the empirical data necessary to construct actuarial tables (in part this is true because systems—and hence vulnerabilities—change quickly such that "the past is not a good predictor of the future"). Second, networked information systems are particularly vulnerable to a major disaster that could result in a large number of claims. Accordingly, the cost of re-insurance for cyberinsurers is high. Finally, barriers to entry into the cyberinsurance market reduce competition. One significant barrier to entry is that a catastrophic event could occur before an insurer has "built up sufficient cash reserves" to pay out on its policies. CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY, *supra* note 493; Press Release, Eur. Network Info. Sec. Agreement, ENISA Report Calls for Kick-Start in Cyber Insurance Market (June 29, 2012), *available at* http://www.enisa.europa.eu/media/press-releases/enisa-report-calls-for-kick-start-for-kick-start-in-cyber-insurance-market ("[To date,] obstacles to the development of an effective cyber insurance market have included lack of actuarial data on the extent of the risk and uncertainty about what type of risk should be insured against.").

497. *CF Disclosure Guidance*, *supra* note 288.

498. *Id.*

499. *See* Perlroth, *supra* 495 (reporting an insurance broker's prediction that cyberinsurance premiums could grow by fifty percent in the twelve to eighteen month period starting in January 2012).

500. Elizabeth Wasserman, *SEC Urged to Give Stronger Guidance on Cyber Disclosure*, BLOOMBERG, (Apr. 10, 2013, 9:57 AM), http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html.

cybersecurity liability where industry has made a reasonable effort to conform to insurer-adopted best practices); (2) private insurers cover industry losses; and (3) the government offers backstop reinsurance for cyberinsurers to help reduce the price of cyberinsurance, thereby improving private sector access to cyberinsurance, and, arguably, leading to improved cybersecurity.[501]

Others have suggested that the federal government use its market power to promote cyberinsurance by requiring its contractors and subcontractors to carry cyberinsurance.[502] This approach would directly increase demand for cyberinsurance. Moreover, companies that purchase cyberinsurance to meet federal contracting requirements presumably would tout their coverage as a competitive advantage when bidding on private contracts, thereby putting pressure on their competitors to purchase cyberinsurance. Accordingly, some argue that this approach would ultimately bring about improved security, more insured companies, and, potentially, reduced costs for insurance coverage.[503] To the extent that development of an insurance market leads to improved security, one might view insurance as part of a holistic vulnerability mitigation strategy, but, at the end of the day, insurance largely is a form of consequence management—a means by which companies manage the consequences of cyberintrusions—and will not, by itself, stop cyberintrusion.

Basic hygiene, improved situational awareness, and maturation of the cyberinsurance market all contribute to vulnerability mitigation, yet vulnerability mitigation alone will not solve the U.S. cybersecurity problem.

B. Beyond Vulnerability Mitigation

The prevailing approach to cybersecurity in the U.S. has been vulnerability mitigation, but the rapid emergence of cyberespionage and cyberattacks as long-term threats to U.S. economic and national security necessitates a serious reevaluation of the private sector's role in cybersecurity as well as U.S. cybersecurity policy. Determined adversaries will find a way to successfully breach even the most sophisticated and heavily fortified organizations, as demonstrated by the successful attacks on DoD, RSA, Lockheed Martin, and Google. Simply throwing money at the cybersecurity problem and attempting to build higher fences around important corporate networks is not proving itself to be a workable long-term solution for U.S. industry, as the above-mentioned Bloomberg study

501. CYBER-INSURANCE METRICS AND IMPACT ON CYBER-SECURITY, *supra* note 493, at 4–5.

502. *Id.* at 3.

503. *Id.* at 5.

suggests.[504] Nor can corporations afford to rely solely on law enforcement efforts to track down and bring perpetrators to justice, as law enforcement is "overwhelmed" by the problem,[505] and hindered by a host of jurisdictional and other issues.[506]

The private sector should give serious consideration to potential options for threat deterrence. As the private sector shifts from a "perimeter defense" to a "threat intelligence" model, it simultaneously should explore the feasibility of "active defense"[507] and other innovative approaches to cybersecurity threats. The spectrum of "active defense"[508] ranges from "modest steps to distract and delay a hacker"[509] to more controversial

---

504. Engleman & Strohm, *supra* note 481.

505. Stewart Baker et al., *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/ ("Cybercrime has cost consumers and banks billions of dollars. Yet few cyberspies or cybercriminals have been caught and punished. Law enforcement is overwhelmed both by the number of attacks and by the technical unfamiliarity of the crimes."); Tim Wilson, *Companies Should Think About Hacking Back Legally, Attorney Says*, DARK READING (Nov. 1, 2012, 7:45 AM), http://www.darkreading.com/risk-management/167901115/security/security-management/240012675/companies-should-think-about-hacking-back-legally-attorney-says.html ("Calling law enforcement doesn't help—they are simply overwhelmed with other cases."); Ellen Nakashima, *Several Nations Trying to Penetrate U.S. Cyber-Networks, Says Ex-FBI Official*, WASH. POST (Apr. 18, 2012), http://articles.washingtonpost.com/2012-04-18/world/35451842_1_cyber-private-sector-networks (" 'I know a lot of companies have suffered, and they are going to want to see somebody come in and assist them,' said [Shawn] Henry, former executive assistant director of the FBI's Criminal, Cyber, Response and Services Branch. 'It won't be the U.S. government . . . . so it's going to have to be the private sector.' ").

506. SANS INST., *supra* note 473, at 7–8.

507. The concept of "active defense" stands in contrast to "passive defense" which relies on firewalls, patches, and anti-virus software. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 417, 461 (2012) ("Active defenses are a . . . category of response to cyberattacks and enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system.").

508. *Id.* at 513 (asserting that active defense is not a unitary whole and describing the different aspects of active defense as "detecting, tracing and [mitigative or retributive] counterstriking").

509. The military has been interested in "active defense" for years. *See, e.g.*, John Stanton, *Rules of Cyber War Baffle U.S. Government Agencies*, NAT'L DEF. MAG. (Feb. 2000), http://www.nationaldefensemagazine.org/archive/2000/February/Pages/Rules4391.aspx ("The Air Force Research Lab . . . has in place a number of cyber-defense mechanisms such as false databases made from deception software (available on the Internet) that create a bogus trail for potential hackers."). A TransAttack—or forensic analysis—begins once an attack is detected. As described by an Air Force Research Lab employee, "While the attack is happening we gather the evidence: Who is doing this? Where are they?" *Id.* Today, private sector security companies offer "active defense" approaches, including deception, to their clients. Liam Tung, *CrowdStrike Boss Explains Offensive Security in Targeted Attacks*, CSO (Aug. 9, 2012,

measures,[510] the legality of some of which may be unclear under today's laws. Some examples of active defense include:

> First, installing honeypots, fake networks and fake documents to slow the attackers down, leave them confused, and perhaps provide the defenders an early warning that the outer walls have been breached. Second, building 'beacons' into your documents, so when they're stolen and opened by the attackers, the documents phone home, telling you not only that you've been compromised, but [also] maybe something about the guys who did it.[511]

Finally, the private sector should consider how to change the .com cybersecurity debate in Washington, which has long-focused on vulnerability mitigation. For political and other reasons, today's debate remains focused on information sharing and voluntary standards, which, according to some experts, may be helpful only "in the margins."[512] The

---

11:44 AM), http://www.cso.com.au/article/433128/crowdstrike_boss_explains_offensive_security_targeted_attacks/ ("[Companies are increasingly demanding] deception, denial, disruption. They're moving more into the government mindset of deception. [Imagine, hypothetically, that] somebody breaks in and steals the plans [for Norththrop Grumman's B-2 Stealth Bomber.] [B]ut if the plans are wrong and the thing doesn't fly, think about the cost of that [to the adversary].").

510. "Hackback" is at the more aggressive end of the "active defense" spectrum, and an animated debate is raging among the cyber-elite over its legality as well as its advisability as a matter of policy. *See* Stewart Baker, *RATs and Poison: Can Cyberespionage Victims Counterhack?*, SKATING ON STILTS (Oct. 13, 2012), http://www.skatingonstilts.com/skating-on-stilts/2012/10/us-law-keeps-victims-from-counterhacking-intruders.html (making a policy case for counterhacking); Stewart Baker, *RATs and Poison II – The Legal Case for Counterhacking*, VOLOKH CONSPIRACY (Oct. 14, 2012, 2:51 pm), http://www.volokh.com/2012/10/14/rats-and-poison-ii-the-legal-case-for-counterhacking/ (making the legal case for counterhacking); Baker et al., *supra* note 505 (debating on legal and policy grounds the following questions: "Can the victims of hacking take more action to protect themselves? Can they hack back and mete out their own justice?"); *see also* Patrick Lin, *'Stand Your Cyberground' Law: A Novel Proposal for Digital Security*, THE ATLANTIC (Apr. 30, 2012, 12:59 PM) http://www.theatlantic.com/technology/archive/2012/04/stand-your-cyberground-law-a-novel-proposal-for-digital-security/256532/; Taylor Armerding, *Should Best Cybercrime Defense Include Some Offense?*, NETWORK WORLD (June 20, 2012, 7:50 AM), http://www.networkworld.com/research/2012/061912-should-best-cybercrime-defense-include-260345.html; Wilson, *supra* note 505 ("Hacking back should never be a company's first response, but in the case of a persistent attacker, it might be the only answer. 'You might be spending $50,000 to $100,000 a week to battle a persistent threat' [attorney David Willson] says. 'You've tried all of the traditional approaches.' ").

511. Stewart Baker, *Taking the Offense to Defend Networks,* STEPTOE CYBERBLOG (June 19, 2012), http://www.steptoecyberblog.com/2012/06/19/taking-the-offense-to-defend-networks/; *see* Wilson, *supra* note 505.

512. Ellen Nakashima, *Cybersecurity Should Be More Active, Official Says*, WASH. POST (Sept. 16, 2012), http://articles.washingtonpost.com/2012-09-16/world/35494752_1_top-cyber-private-sector-crowdstrike (quoting Steven Chabinsky, former Deputy Assistant Director of the FBI's Cyber Division and current

private sector should urge Congress to broaden the debate to include consideration of the private sector's potentially game-changing role in threat deterrence. The private sector should urge Congress to remove barriers to private sector efforts to develop innovative approaches to threat deterrence. The private sector simultaneously should urge the government to bring all elements of national power—including economic,[513] diplomatic,[514] and military[515]—to bear to deter would-be threat actors.

Senior Vice President of Legal Affairs and Chief Risk Officer at CrowdStrike).

513. On the economic front, the private sector could, for example, press for greater domestic legal protections from the threat of economic espionage, potentially including penalties for those Chinese companies benefitting from industrial espionage. This would be a natural extension of the U.S.-China Economic and Security Review Commission recommendations that Congress "conduct a review of existing legal penalties for companies found to engage in, or benefit from, industrial espionage." U.S.-CHINA ECON. & SEC. REV. COMM'N, *supra* note 186, at 188; *see* Gerald O'Hara, Comment, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 244 (2010) (discussing the Economic Espionage Act and concluding that "current law is inadequate to deal with the cybertheft of corporate trade secrets"). Others have suggested that the United States use the Committee on Foreign Investment in the United States ("CFIUS") approval process for leverage. *See* Stewart Baker, *More on Cybersecurity and Attribution: Si Chuan University and Tencent*, STEPTOE CYBERBLOG (Dec. 5, 2012), http://www.steptoecyberblog.com/2012/12/05/more-on-cybersecurity-and-attribution-si-chuan-university-and-tecent/. CFIUS is the "inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person . . . in order to determine the effect of such transactions on the national security of the United States." *See Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF THE TREAS. RES. CTR., http://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx (last updated Dec. 20, 2012, 1:37 PM).

514. The administration recently stepped up efforts to address the threat of Chinese cyberespionage through diplomatic channels, beginning with National Security Advisor Tom Donilon's speech at the Asia Society. Donilon, *supra* note 213 ("Specifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace . . . ."). *See also infra* Section IV.B.5. However, much work remains to be done. On the diplomatic front, the United States can act through a variety of channels, potentially including the WTO, to penalize companies that benefit from industrial espionage and to "discourage foreign countries from enabling or tolerating cyberespionage." O'Hara, *supra* note 513, at 274 ("[T]he President should instruct the United States Trade Representative to engage strategic allies to coauthor a resolution decrying the use of cyber attacks to misappropriate proprietary economic information. There are many countries in both the developed and developing blocs that have much to lose through cyber-espionage attacks, and using the WTO as a vehicle to navigate change on intellectual property protection has been successful in the past.").

515. The United States needs to continue to develop its military strategy for deterring cyberattacks. General Alexander's public testimony on March 12, 2013 clearly plays into such a strategy by identifying the capabilities CyberCom is

With these actions, it is hoped that the fiddlers on the roof will "[keep their] balance . . . for many, many years"[516] to come.

developing and how they are to be used. Specifically General Alexander told Congress that he is developing "an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace" and that "[t]hirteen of the teams that [the Pentagon is] creating are for that mission alone." Mazzetti & Sanger, *supra* note 223; Richard Lardner, *Pentagon Forming Cyber Team to Prevent Attacks*, PHYS.ORG (March 12, 2013), http://phys.org/news/2013-03-deters-major-cyberattacks.html#jCp ("Alexander told the Senate Armed Services Committee that foreign leaders are deterred from launching cyberattacks on the United States because they know such a strike could be traced to its source and would generate a robust response."). Alexander's comments certainly appear to have been designed to serve a deterrence function. *See generally* Jack Goldsmith, *The Significance of Panetta's Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks*, LAWFARE (Oct. 15, 2012, 1:26 PM), http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/ (discussing then-Defense Secretary Panetta's speech and suggesting that "the speech's real significance . . . concerns DOD's evolving deterrence posture . . . . Panetta had two main messages related to deterrence. [First,] '[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.' Second, . . . he makes plain that the DOD has the capabilities and desire to engage in a *preemptive* attack[] against *imminent* cyber threats.") (emphasis in original). *See* Charles L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security*, GEO. WASH. UNIV. CYBER SECURITY POL'Y AND RES. INST. 6 (2011) http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf ("Deterring cyber attacks may not be as difficult as the emerging conventional wisdom suggests. . . . To support its deterrence policy, the United States needs a clear declaratory policy that lays out its plans for responding to various types of attacks.").

516. FIDDLER ON THE ROOF, *supra* note 1.

RELIANCE ON EXPERTS FROM A CORPORATE LAW PERSPECTIVE

ALEXANDROS N. ROKAS*

In discharging their duty of care, directors of corporations are not expected to independently investigate all parameters affecting a decision they are about to make. In fact, statutory provisions encourage or sometimes require directors to seek the advice of experts, such as auditors, lawyers, investment bankers, and tax specialists. In this Article, emphasis is placed on Section 141(e) of the Delaware General Corporation Law, according to which directors are entitled to rely on the advice of such experts as long as they believe that the advice was within the expert's professional competence, the expert was selected with reasonable care, and reliance is in good faith. Apart from systematizing the elements of this rule, as they were interpreted by a significant number of court decisions, this Article sheds light on the interaction of the reliance defense with basic concepts of Delaware corporate law, mainly the business judgment rule, as well as good faith, after Caremark. *This Article does not examine whether directors will be eventually held liable (which, besides, is rarely the case in Delaware due to the business judgment presumption, exculpatory clauses, and insurance and indemnification provisions), but solely whether the additional defense of Section 141(e) should apply or not.*

* LL.M., *Harvard Law School, Fulbright* and *Onassis Scholar*, 2011–12; Ph.D., *Humboldt University of Berlin*; LL.B., *University of Athens*, admitted in Athens, Greece. The author would like to thank Professor Reinier H. Kraakman and the participants of the Comparative Corporate Governance Seminar for their constructive feedback and comments.

TABLE OF CONTENTS

INTRODUCTION: PSYCHOLOGY OF DECISION-MAKERS AND CORPORATE LAW

Decision-making is often a painful process. Decision-makers face various challenges, ranging from lack of factual data or incapacity to critically assess the available data to an unwillingness to undertake responsibility or personal conflicts of interest. Many challenges appear in periods of uncertainty, such as during financial and other crises. In such periods, decision-makers would feel extremely relieved if somebody else could bear the burden and offer an answer to whatever dilemma they are facing. They would feel even more comfortable if they knew that relying on this advice would remove the burden of responsibility, in case the

advice proves to be wrong.[1]

To be sure, feeling more secure is not per se harmful. However, turning the decision-making process into a process of uncritical adoption of a third-party's view could seriously distort the intellectual element involved in this process. Even if the advice is sound, decision-makers may not be able to oversee the implementation of their decision in the future and will fail to adjust their strategy in the absence of the advisor. In fact, a relatively recent empirical experiment examined the neurobiological processes of making financial decisions with and without expert advice, especially under conditions of enhanced uncertainty.[2] It showed that areas of the brain responsible for making value judgments, accessible through Magnetic Resonance Imaging ("MRI") technology, were clearly less active when such advice was received. This result was not affected by the fact that the financial advisor's suggestions were very conservative and, thus, could not lead to maximum earnings.[3] The researchers did not examine what caused this behavior; however, one could speculate that the feeling of safety, created by the presence of the (perceived) authority, coupled with the surrounding conditions of uncertainty, and sometimes the laziness of decision-makers, led them to offload the responsibility for making financial decisions. A similar experiment, concentrating on brain activities when choosing and changing financial advisors, concluded that detecting errors of advisors is more likely when the recipients of the advice consider changing their advisors.[4] According to the researchers, in the absence of such circumstances, recipients observe more the personal characteristics of the advisors, and less the numerical realities.

The most prominent personal characteristic of the advisors is their ability to convey trust. This seemed to be the case, for instance, with the relationship of members of various Wisconsin school boards and David W. Noack, who, in 2006, convinced them to borrow more than $160 million

---

1. Of course, in most cases the latter is not possible because the one suffering the consequences of incorrect advice is the decision-maker himself. A patient trusting his doctor would damage his health if the medication the doctor provided is improper. In the case of fiduciaries, though, decisions affect third persons. Corporations form the most prominent example because directors administrate "other people's money," an expression introduced in LUIS BRANDEIS, OTHER PEOPLE'S MONEY AND HOW BANKERS USE IT (1914).

2. *See* Jan B. Engelmann et al., *Expert Financial Advice Neurobiologically "Offloads" Financial Decision-Making under Risk*, PLOS ONE (Mar. 24, 2009), http://www.plosone.org/article/info:doi%2F10.1371%2Fjournal.pone.0004957.

3. *See id.*

4. Russell N. James III, *Choosing and Changing Financial Advisors: An fMRI Study of Associated Brain Activations* 1 (Working Paper, Feb. 27, 2012), *available at* http://www.researchgate.net/publication/228293349_Choosing_and_Changing_Financial_Advisors_An_fMRI_Study_of_Associated_Brain_Activations.

and contribute $35 million of their own money to purchase synthetic collateralized debt obligations ("CDOs") sold by the Royal Bank of Canada ("RBC").[5] Noack, apart from being an investment banker who provided decades-worth of services to the schools, was also the son of a teacher who taught at a local school for forty-seven years, while all of his children attended local schools. With regard to the investment, Noack stated that "[t]here would need to be 15 Enrons" for the schools to lose money.[6]

At the same time, some of the challenges mentioned at the beginning of this Article were present. First, due to the complexity of the proposed investment, the board members lacked sufficient knowledge to independently assess its details. One of the members, who was a financial advisor himself, admitted he never read the thick packets of documents he received, claiming that he was not worried because the board had its questions satisfactorily answered by Noack. Second, Noack's company, Stifel, Nicolaus & Company ("Stifel"), had close ties with RBC. Finally, board members never examined the advisor's qualifications relating to such investments, which were in fact limited. This confirms the trust element of the board's relationship to Noack.[7] The rest of the story is more or less predictable: the CDOs lost most of their value, and the Securities and Exchange Commission ("SEC") charged Stifel and RBC with fraudulent misconduct.[8]

Corporate boards, like school boards, consist of fiduciaries entrusted with the administration of an estate. However, they more often have to reach investment decisions or decisions on other complicated issues that require an expert's advice. On the other hand, corporate board members tend to be more qualified than school board members for such purposes, and a substantial body of statutory provisions facilitates the decision-making process. In this Article, emphasis is given to corporate law provisions enabling corporate board members under certain conditions to trust their advisors and escape liability should the advice prove to be mistaken. After explaining the reasoning behind the relevant rules in Delaware law (Section I), this Article unfolds all elements included in the relevant provision (Section II), as well as further requirements set by case law and recommended by scholars (Section III). Final conclusions are

5. *See* Charles Duhigg & Carter Dougherty, *The Reckoning: From Midwest to M.T.A., Pain From Global Gamble*, N.Y. TIMES (Nov. 1, 2008), http://www.nytimes.com/2008/11/02/business/02global.html?pagewanted=all.

6. *Id.*

7. *Id.* Of course, it was not only trust that led to the board's decision. CDOs were quite popular at that time, and the particular CDOs received satisfactory ratings.

8. *See* Press Release, SEC, SEC Charges RBC Capital Markets in Sale of Unsuitable CDO Investments to Wisconsin School Districts (Sept. 27, 2011), *available at* http://www.sec.gov/news/press/2011/2011-191.htm.

offered at the end of this Article.

I. THE RULE AND ITS JUSTIFICATION

In Delaware, the key provision enabling boards to rely on their advisors is Section 141(e) of the Delaware General Corporation Law ("DGCL"), which states:

> A member of the board of directors, or a member of any committee designated by the board of directors, shall, in the performance of such member's duties, be fully protected in relying in good faith upon the records of the corporation and upon such information, opinions, reports or statements presented to the corporation by any of the corporation's officers or employees, or committees of the board of directors, or by any other person as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care by or on behalf of the corporation.[9]

The legislative history of Section 141(e) shows that its initial version, as adopted in 1943, did not encompass all categories of outside experts, but only public accountants and appraisers.[10] In fact, it took some decades for the state legislators to broaden the language of the provision: in 1974, Section 35 of the Model Corporation Act was amended to include all sorts of experts.[11] Subsequently, many states (including Delaware in 1987) adopted similar provisions.[12]

Even before 1974, directors throughout the United States relied on outside advisors, and courts recognized this reliance as a factor that must be considered in assessing good faith. For example, in 1936, the Michigan Supreme Court (applying Delaware law) dealt with the case of a director who, based on advice provided by his counsel, approved certain dividends, rendering the company insolvent.[13] The legality of the dividends was questionable because they were declared from monies received from the

---

9. DEL CODE ANN. tit. 8, § 141(e) (2010). There is a similar provision in Section 172, regulating the reliance on experts with regard to "facts pertinent to the existence and amount of surplus or other funds from which dividends might properly be declared and paid." *See id.* § 172.

10. *See* 44 Del. Laws 423 (1943) (stating that a director "shall in the performance of his duties be fully protected in relying in good faith upon . . . reports made to the corporation by any of its officials, or by an independent certified public accountant, or by an appraiser selected with reasonable care by the Board of Directors").

11. *Report of Committee on Corporate Laws: Changes in the Model Business Corporation Act*, 30 BUS. LAW. 501 (1974–75).

12. *See* 66 Del. Laws 335 (1987); MODEL BUS. CORP. ACT ANN., § 8.30, at 8-207 (2011).

13. *See* Stratton v. Anderson, 270 N.W. 764, 764 (Mich. 1936).

sale of certain territorial franchise rights.[14] The court did not hesitate to adopt a broad exception to liability, stating that evidence proving advice "not only . . . negat[es] any bad faith upon the part of defendant in voting for the dividend following the receipt of this advice, but it [also] sanctions a finding by us that such vote was made in good faith and without negligence."[15] Facts indicating reliance were taken into account by courts in numerous cases outside corporate law—ranging from criminal to tax cases—as elements supporting good faith.[16]

Behind this finding lies a basic justification of the reliance doctrine, namely that it is in accordance with the principles of prudent decision-making. The above-mentioned decisions support the view that even in the absence of a reliance provision, reliance is a fact to be taken into account to determine whether directors acted with due care and in good faith.[17] Generally, seeking advice indicates a reasonable effort of the director to become informed and gain the necessary familiarity with complicated facts in the course of the decision-making process. Reliance does not contradict the business judgment rule. One of the requirements of this rule is to reach *informed* decisions. This is generally deemed to be satisfied when the director consults and relies on outside professionals.[18]

The argument for reliance provisions invites us to admit that directors are not capable of independently assessing all relevant and available facts or personally contacting every officer and employee in order to become informed. Solely reading written reports of the various divisions of the corporation would require an enormous amount of time, especially in large

14. *See id.* at 766–67.

15. *Id.* at 767; *see also* Smith v. Van Gorkom, 488 A.2d 858, 881 (Del. 1985). *See generally* Thomas L. Preston, *Advice of Counsel as a Defense*, 28 VA. L. REV. 26 (1941).

16. *See* Douglas W. Hawes & Thomas J. Sherrard, *Reliance on Advice of Counsel as a Defense in Corporate and Securities Cases*, 62 VA. L. REV. 1, 9–11 (1976).

17. One would expect that common law countries would not include reliance provisions, leaving the interpretation of duty of care issues to the courts. While the United States, Australia (see *infra* note 63), and New Zealand have such provisions, Germany and other civil law countries do not. Recently, the German Federal Court of Justice ("BGH") set the conditions under which boards can rely on legal advisors based on the general duty of care provision. Bundesgerichtshof [BGH] [Federal Court of Justice] Sept. 20, 2011, II ZR 234/09. These conditions are quite similar to the ones detailed in this Article, while the legal literature (before the decision was issued) regularly refer to relevant U.S. concepts. *See, e.g.*, Holger Fleischer, *Vertrauen von Geschäftsleitern und Aufsichtsratsmitgliedern auf Informationen Dritter*, 30 ZEITSCHRIFT FÜR WIRTSCHAFTSRECHT 1397 (2009).

18. *See* A.L.I., PRINCIPLES OF CORPORATE GOVERNANCE, § 4.01(c) cmt. b, 171 (1994); *see also Van Gorkom*, 488 A.2d at 873 (noting that "gross negligence" is the appropriate standard to apply when evaluating whether directors were adequately informed in reaching a business judgment).

corporations. "Directors would be snowed under with paper," as one commentator puts it, while directorship would become an extremely hazardous job.[19] In such corporations, the hierarchy structure and the distinct roles assigned are crucial factors affecting the efficiency and the pace of decision-making. Roles are usually assigned in accordance with the significance of decisions, which brings to mind again certain duty of care interpretations, according to which the importance of the business judgment to be made is a factor affecting the reasonable investigation directors are required to perform.[20] Therefore, by providing a safe harbor, directors and officers are encouraged to introduce such organizational structures that expedite and rationalize the decision-making process, while at the same time honoring their duty of care.[21]

On the other hand, critics could allege that reliance provisions encourage wrongful conduct, motivating directors to shield themselves behind the advice given without actually familiarizing themselves with the decision to be made or, even worse, knowing its negative aspects. Reliance provisions may even incentivize directors to shop for favorable advice.[22] However, as Section 141(e) implies, and as will be explained below, courts should consider all factors calling into question the good faith of the decision-makers. Thus, rejecting unfavorable advice could indicate bad faith, excluding the application of the rule. The mere fact that the board hired an advisor and adopted his views does not constitute an absolute defense when good faith is questioned. To the extent that Section 141(e) excuses negligent behavior, as will be explained below, criticism is justified.[23]

II. STATUTORY ELEMENTS OF THE RULE

A. Stricto Sensu *Reliance*

The first element of the reliance doctrine is self-explanatory: there is no reliance and the directors will not enjoy the protection of Section 141(e) if they do not follow the advice provided in all its material aspects.[24]

---

19. Robert W. Hamilton, *Reliance and Liability Standard for Outside Directors*, 24 WAKE FOREST L. REV. 5, 19 (1989).

20. *Id.*

21. R. Franklin Balotti & Megan W. Shaner, *Safe Harbor for Officer Reliance: Comparing the Approaches of the Model Business Corporation Act and Delaware's General Corporation Law*, 74 J. L. & CONTEMP. PROBS. 161, 170 (2011) (referring to officers).

22. *See* Hawes & Sherrard, *supra* note 16, at 8.

23. *See infra* Section III.A.

24. *See* Brehm v. Eisner, 746 A.2d 244, 262 (Del. 2000); Ash v. McCall, No. Civ. A. 17132, 2000 WL 1370341, at *9 (Del. Ch. Sept. 15, 2000); Hawes & Sherrard, *supra* note 16, at 35; Thomas A. Uebler, *Reinterpreting Section 141(e) of Delaware's General Corporation Law: Why Interested Directors Should Be Fully Protected in*

Directors are not required to accept the recommendations of the experts; however, if they do not follow the advice, they will not be able to invoke the protection of Section 141(e). Regardless, unless gross negligence is proven, directors are still shielded by the business judgment presumption, since the latter is a broader shield for directors and applies even when Section 141(e) is inapplicable.[25] Consequently, not following the advice does not necessarily indicate bad faith or negligence, but merely excludes the applicability of the reliance doctrine.[26] Seen from this perspective, the Delaware Court of Chancery in *In re Walt Disney Co. Derivative Litigation* misinterprets Section 141(e) in saying that:

> [a]n interpretation of Section 141(e) that would require boards to follow the advice of experts (substantially? completely? in part?) before being able to claim reliance on those experts would be in conflict with the mandate in Section 141(a) that the corporation is to be managed 'by or under the direction of a board of directors.'[27]

There are cases, where, for various reasons, following the advice of experts is not a simple task. Such cases occur when a legal opinion concludes that a particular course of action is "more likely permissible than not,"[28] when it provides for more than one option, or when the recipient of the advice fails to understand the means of its implementation. In these instances, what matters is the director's effort to make sure his actions comply with the advice and, if necessary, ask for further explanation. If he fails to do so, reliance will not be granted.

B. Reliance in Good Faith

Without the requirement of good faith, reliance provisions would be a shelter for incompetent or even dishonest directors to hide behind the advice of an outside advisor. Good faith is a broad concept that refers mainly to the state of mind of the directors who claim reliance. Therefore, by definition, it covers most cases of dishonest directors. The violation of the good faith requirement does not lead to director liability, but only to the inapplicability of the reliance doctrine.

The general notion applies that a conscious (or intentional) disregard of

---

Relying on Expert Advice, 65 BUS. LAW. 1023, 1045 (2010).

25. *Ash*, 2000 WL 1370341, at *9 ("[A board of directors] is entitled to the presumption that it exercised proper business judgment, including proper reliance on experts."); *see also infra* Section III.A.4.ii.

26. *Contra* Hawes & Sherrard, *supra* note 16, at 35.

27. *In re* Walt Disney Co. Derivative Litig., 907 A.2d 693, 770 n.550 (Del. Ch. 2005), *aff'd*, 906 A.2d 27 (Del. 2006).

28. *See* Hawes & Sherrard, *supra* note 16, at 33.

the director's duties constitutes bad faith. The Model Business Corporation Act ("MBCA") entitles a director who does not have "knowledge that makes reliance unwarranted" to rely on experts.[29] Even though there is no reference to the concept of good faith, the MBCA's requirement is largely equivalent to the good faith requirement, perhaps with a stronger emphasis on the subjective elements of the director's behavior.[30] An example of knowledge that would make reliance unwarranted is being aware of facts that contradict the findings of the expert.[31] For example, there is a lack of good faith if the director knows—due to his personal expertise or due to a tip provided by an employee—that the advice is shoddy, or if he adopts only favorable advice and rejects other experts' opinions.[32] In such cases, the director should disclose these facts to the rest of the board according to MBCA Section 8.30(c).[33] Other instances of bad faith will be discussed later in this Article.[34]

---

29. MODEL BUS. CORP. ACT § 8.30(e). *But see* N.Y. BUS. CORP. LAW § 717(a) (McKinney 2003 & Supp. 2013) ("[A director] shall not be considered to be acting in good faith if he has knowledge concerning the matter in question that would cause such reliance to be unwarranted.").

30. The content of good faith, in particular whether it encompasses only subjective or also objective components is a disputed issue. *See* E. Norman Veasey & Christine T. DiGuglielmo, *What Happened in Delaware Corporate Law and Governance from 1992-2004? A Retrospective on Some Key Developments*, 153 U. PA. L. REV. 1399, 1452–53 (2005).

31. *See* Hamilton, *supra* note 19, at 21.

32. *See In re* Emerging Commc'ns, Inc. S'holders Litig., No. 16415, 2004 WL 1305745, at *38–43 (Del. Ch. June 4, 2004) (holding—without citing Section 141(e)—that a director possessing special financial expertise did not reasonably rely on a fairness opinion, because he had very strong reasons to suspect that the price was unfair and that he should not vote in favor of the proposed transaction). Corporations hire skilled directors to take advantage of their expertise. In another decision, the same court concludes that even "board members who are experts are fully protected under § 141(e) in relying in good faith on the opinions and statements of the corporation's officers and employees who were responsible for preparing the company's financial statements," adding that plaintiffs should "plead with particularity facts that would lead to the reasonable inference that the director defendants made or allowed to be made any false statements or material omissions with knowledge or in bad faith." *In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 135 (Del. Ch. 2009). This concept is rather confusing; one should conclude, however, that even after *Citigroup*, courts should examine the good faith of skilled directors and take into account their particular qualifications and exposure.

33. *See* MODEL BUS. CORP. ACT § 8.30(c) ("In discharging board or committee duties a director shall disclose . . . to the other board or committee members information not already known by them but known by the director to be material to the discharge of their decision-making or oversight functions . . . .").

34. *See infra* Section III.A.

C. Reasonable Belief That the Advice Was Within the Expert's Professional Competence

The language of Section 141(e) shows that the rule applies even if the expert opines on a subject not within his area of competence as long as the director reasonably believes the opposite (and the rest of the provision's requirements apply). This will occur only in extreme cases because reasonableness must be assessed in an objective manner—that is, based on material information that was reasonably available about the expert.[35]

In assessing whether there is a reasonable belief that an expert acts within his professional competence, all factors should be taken into consideration. For instance, a lawyer would be suitable to opine on technical issues of environmental compliance if he specializes in environmental law or if he is member of a legal organization with access to relevant information and it is not the first time he deals with compliance.[36] In the case of *Selectica, Inc. v. Versata Enterprises*, the Delaware Court of Chancery considered an investment banker suitable to assess the value of net operating losses ("NOLs") and to explain the consequences of a potential sale.[37] The court placed emphasis on the fact that the Board had "ample cause to consider him an expert qualified to speak on Selectica's NOLs and on the threat of their impairment," taking into account inter alia his work history as a tax attorney and partner at several accounting firms.[38] On the other hand, a lawyer is generally not the appropriate person to opine on questions of fact, such as valuation and fairness issues.[39] In such cases, there should be two opinions, one for the facts, and one for the legal issues based on the facts presented in the first opinion.

D. Selection with Reasonable Care

The requirement of reasonably believing that the advice is within the expert's professional competence and the requirement of selecting the expert with reasonable care are partially interchangeable as a careful selection excludes experts that the director believes are incompetent. Apart from that, a careful selection process should eliminate experts that are not

35. *See* Uebler, *supra* note 24, at 1042 ("objective reasonableness").

36. *See* MODEL BUS. CORP. ACT ANN. § 8.30, at 8-204.

37. *See* Selectica, Inc. v. Versata Enters., No. 4241-VCN, 2010 Del. Ch. LEXIS, at *50 (Mar. 1, 2010).

38. *Id.*

39. *See* Glassberg v. Boyd, 116 A.2d 711, 719 (Del. Ch. 1955); *see also* Valeant Pharms. Int'l v. Jerney, 921 A.2d 732, 751 (Del. Ch. 2007) (acknowledging that outside legal advisors can opine on whether a proposed transaction will be subject to the entire fairness test and on the possible outcomes of the test, but not on the actual substantive fairness of the proposal); Bevis Longstreth, *Reliance on Advice of Counsel as a Defense to Securities Law Violations*, 37 BUS. LAW. 1185, 1194 (1982).

reliable due to factors of personal nature. Such factors relate to the bias of the advisors, and, secondarily, to instances of frivolous or unprofessional behavior on the part of the expert. This Section will mainly cover conflict of interest issues as competence issues are discussed above.[40]

Conflicts of interest arise primarily when the independence and objectivity of the expert are questionable. An obvious example: in the context of leveraged buy-outs ("LBOs"), allowing the acquirer to select an appraiser for a solvency opinion can easily render the selection process flawed.[41] Similarly, if Company X is about to acquire substantial assets of Company Y, the director of Y, who also owns X, is not suited to appoint the advisor to this transaction.[42] The mere fact that management selected the advisor, though, is insufficient to prove a conflict of interest.[43] If management had a conflicting interest in the transaction that is known to the board, directors should avoid trusting their advisors. For example, in *Valeant Pharmaceuticals International v. Jerney*, the Delaware Court of Chancery examined the fairness of bonuses paid to former directors and officers after a spin-off of a division of the company.[44] The board of directors instructed the compensation committee to select a particular advisor, who had already issued an opinion favoring the award of bonuses, instead of selecting its own independent compensation consultant.[45] The court decided to deny the application of reliance provisions.[46]

---

40. *See supra* Section II.C.

41. *See, e.g.*, Brandt v. Hicks, Muse & Co. (*In re* Healthco Int'l, Inc.), 208 B.R. 288, 307 (Bankr. D. Mass. 1997) (adding that the opinion was based on the data provided by the acquirer and thus some losses were understated).

42. Boyer v. Wilmington Materials, Inc., 754 A.2d 881, 910 (Del. Ch. 1999) (finding that Section 141(e) is not a defense).

43. *Cf.* James D. Cox, *Managing and Monitoring Conflicts of Interest: Empowering the Outside Directors with Independent Counsel*, 48 VILL. L. REV. 1077, 1086–87 (2003) (citing cases showing that, in the absence of signs of self-dealing, plaintiffs' claims alleging that advisors were not independent from senior management usually get dismissed).

44. 921 A.2d 732 (Del. Ch. 2007).

45. Further flaws in the procedure included the fact that the advisor based his opinion on misleading information provided by management, that his report addressed a different transaction from the one actually adopted, and that some of the committee's members were interested in the transaction. *Id.* at 748, 751.

46. *Id.* at 751. Interestingly, the court did not just hold Section 141(e) inapplicable, but added that in entire fairness cases, the existence of reasonable reliance, while being a factor in evaluating whether directors have met the standard of fairness, is not "outcome determinative of entire fairness" because this would replace the court's role in determining entire fairness under Section 144 and would create a conflict between Sections 141(e) and 144. In response to this view, Thomas A. Uebler notes that a court should first assess the entire fairness of the transaction (and, in doing so, consider various factors, among which is the use of advisors). Then, if the transaction has been found to be unfair, the court should consider the Section 141(e) defense. Applying this theory to the *Valeant* facts, and assuming that the transaction was found to be unfair,

Delaware courts have assessed transactions in which advisors had a personal stake in a business transaction. In *In re Del Monte Foods Co. Shareholders Litigation*, the court found that a financial advisor misled the board of a company that private equity buyers were in the process of acquiring.[47] The advisor did not disclose to the board that the advisor would participate in the buy-side financing and that the advisor actually encouraged potential buyers even before its appointment as advisor.[48] The board was unaware of the advisor's interactions with the potential buyers. The court examined the breach of fiduciary duties for the purpose of granting injunctive relief to delay the shareholder vote and did not examine monetary liability, admitting that Sections 102(b)(7)[49] and 141(e) make the chances of a judgment for money damages "vanishingly small."[50] In other words, the Court implied that Section 141(e) applies despite the advisor's interest in the transaction. This makes sense because undisclosed facts the board could not have known do not undermine the reasonableness of the Section 141(e) selection process.[51] To require that boards ask advisors to disclose any conflicts of interest would exceed the reasonable inquiry a board must make and render the Section 141(e) selection process highly unpredictable. Requiring that boards ask advisors to disclose conflicts of interest could eliminate, of course, the risk of injunctive relief.[52] Finally,

---

but Section 141(e) applied, the directors would have been required to disgorge the unfair portion of the compensation, but, on the other hand, they would not have been held liable for additional monetary damages flowing from breach of fiduciary duty. *See* Uebler, *supra* note 24, at 1049, 1053. Furthermore, Professor Bainbridge, adopting a somewhat different approach, concludes that the court's view in this case serves to eviscerate Section 141(e), noting that a Section 141(e) report should indeed be "outcome determinative." *See* Stephen Bainbridge, *Eviscerating DGCL 141(e)*, PROFESSORBAINBRIDGE.COM (Apr. 2, 2007), http://www.professorbainbridge.com/professorbainbridgecom/2007/04/eviscerating-dgcl-141e.html.

47. *In re* Del Monte Foods Co. S'holders Litig., 25 A.3d 813 (Del. Ch. 2011).

48. *See id.* at 823 (noting that the board had previously called off the process of a potential sale, and its investment bankers maintained contact with the potential buyers, despite the confidentiality agreement).

49. DEL. CODE ANN. tit. 8, § 102(b)(7) (2011); *see* Ryan *ex rel.* Maxim Integrated Prods. v. Gifford, 2009 Del. Ch. LEXIS 1, at *23–24 n.27 (Del. Ch. Jan 2, 2009) ("Section 102(b)(7) allows companies to adopt a provision in their certificate that eliminates the personal liability of directors for monetary damages for breach of fiduciary duty as a director, except for, among other things, breaches of the duty of loyalty and acts or omissions not in good faith or which involve intentional misconduct.").

50. *See In re Del Monte Foods Co. S'holders Litig.*, 25 A.3d at 818.

51. *See* Brehm v. Eisner, 746 A.2d 244, 262 (Del. 2000) ("[T]he faulty selection process was attributable to the directors."); *see also* Hawes & Sherrard, *supra* note 16, at 25 ("[I]f reasonable inquiry would not have disclosed the interest.").

52. *See* David A. Katz, Del Monte *and the Responsibility of a Board in a Sales Process*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Apr. 14, 2011), http://blogs.law.harvard.edu/corpgov/2011/04/14/del-monte-and-the-responsibility-of-

the court noted that, even if monetary liability is not an option, disgorgement of transaction-related profits may be available as an alternative remedy.[53] This concept agrees with Uebler's above-mentioned concept, according to which the applicability of Section 141(e) does not undermine alternative remedies, such as the disgorgement of amounts received as a result of an unfair transaction.[54]

Another variation of having interest in the transaction arises when a substantial part of the advisor's fee depends on the success of the transaction (contingent fees). Delaware courts hold that the sole presence of such a fee structure does not itself destroy the advisor's perceived independence and that additional factors should be considered.[55] As a practical matter, prominent financial advisors normally would not risk their reputation issuing inaccurate or incomplete advice.[56]

Finally, while courts have sporadically demonstrated a prejudice against the independence of in-house counsels,[57] the reputations of in-house legal departments are rapidly improving.[58] The general rule is that particularized facts indicating bad faith or a flawed selection process are required to rebut the presumption of disinterestedness.[59]

III. FURTHER REQUIREMENTS

Beyond the expressly stated elements of Section 141(e), courts and scholars set additional requirements for the application of the reliance doctrine. Most notably, in *Brehm v. Eisner*,[60] the Delaware Supreme Court tried to systematize all basic requirements, stating that to reject reliance, a complaint must:

> allege particularized facts . . . that, if proved, would show, for example, that: (a) the directors did not in fact rely on the expert; (b) their reliance

---

a-board-in-a-sales-process.

53. *See In re Del Monte Foods Co. S'holders Litig.*, 25 A.3d at 838.

54. *See* Uebler, *supra* note 24.

55. *See In re* General Motors (Hughes) S'holders Litig., No. Civ. A. 20269, 2005 WL 1089021, at *14 n.143 (Del. Ch. May 4, 2005), *aff'd*, 897 A.2d 162 (Del. 2006) (noting that the fee arrangement was unremarkable in terms of the overall value of the transaction).

56. *See* Winters v. First Union Corp., No. 01-CVS-5362, 2001 WL 34000144, at *4 (N.C. Super. Ct. July 12, 2001) (noting further that contingent fee arrangements are standard within the investment banking industry).

57. *See In re* Oracle Secs. Litig., 829 F. Supp. 1176, 1189 (N.D. Cal. 1993) ("inherently biased counsel").

58. Steven L. Schwarcz, *To Make or to Buy: In-House Lawyering and Value Creation*, 33 J. CORP. L. 497, 510 (2008).

59. *See* Hawes & Sherrard, *supra* note 16, at 26.

60. 746 A.2d 244, 262 (Del. 2000).

> was not in good faith; (c) they did not reasonably believe that the expert's advice was within the expert's professional competence; (d) the expert was not selected with reasonable care by or on behalf of the corporation, and the faulty selection process was attributable to the directors; (e) the subject matter . . . that was material and reasonably available was so obvious that the board's failure to consider it was grossly negligent regardless of the expert's advice or lack of advice; or (f) that the decision of the Board was so unconscionable as to constitute waste or fraud.[61]

Requirements (a) through (d) rephrase Section 141(e). The most crucial requirement is (e) because it is the only one directly aimed at preventing the blind adoption of experts' views, which, as noted at the beginning of this Article, poses a significant problem for the reliance doctrine, due to the psychological safety decision-makers seek. This Section will explore further requirements that are thought to rationalize the reliance process. As the wording of the above court decision implies, there is a presumption that these requirements are met, meaning the plaintiff must present contrary evidence.[62]

A. No Blind Reliance

According to the first requirement, the board should not blindly adopt the advice given, i.e. without even trying to understand its basic logic. This concept, though, is somewhat vague. A broad interpretation of this requirement renders the reliance doctrine useless. Requiring, for example, that directors familiarize themselves with all technical aspects of the advice given would doubtlessly deviate from current business practices. Similarly, requiring that they obtain all necessary information to be able to independently assess the substance of the advice would severely undermine the reliance doctrine and impose less than cost-effective duties. Besides, under Delaware law, the sole ground deterring blind reliance can be found in the (somewhat abstract) good-faith limitation incorporated in Section 141(e). Unlike the wording adopted in New York or, more explicitly, in Australian law, there is no further limitation in the discussed statute.[63]

---

61. *Id.*; *see* Ash v. McCall, No. Civ. A. 17132, 2000 WL 1370341, at *9 (Del. Ch. Sept. 15, 2000).

62. *See Ash*, 2000 WL 1370341, at *9 ("The . . . board is entitled to the presumption that it exercised proper business judgment, including proper reliance on experts.")

63. N.Y. BUS. CORP. LAW § 717(a) (McKinney 2003 & Supp. 2010) ("[I]n so relying he shall be acting in good faith *and with such degree of care . . . .*") (emphasis added); *see* Hanson Trust PLC v. ML SCM Acquisition, Inc., 781 F.2d 264, 275 (2d Cir. 1986) (noting that directors have some oversight obligations to become reasonably familiar with an opinion, report, or other source of advice before becoming entitled to rely on it); *see also Corporations Act 2001*, § 189(b) (Austl.) ("[If] the reliance was

1. Smith v. Van Gorkom *on Reliance*

In the past, Delaware case law emphasized this element of the reliance doctrine, notably in the groundbreaking decision *Smith v. Van Gorkom*.[64] At the time, Section 141(e) encompassed only reliance on a corporation's own officials, accountants, and appraisers.[65] According to the court's holding, certain circumstances may give rise to the director's duty to make a "reasonable inquiry" into the reports submitted by officers.[66] In *Van Gorkom*, these circumstances included "hastily calling the meeting without prior notice of its subject matter, the proposed sale of the Company without any prior consideration of the issue or necessity therefor, the urgent time constraints imposed by [a takeover specialist], and the total absence of any documentation whatsoever . . . ."[67] Although the directors had no financial expertise, the court held that they could not reasonably have relied on the reports in good faith if they accounted for all reasonably available information.[68] The board is "entitled to good faith, not blind, reliance."[69]

2. Narrowing Good Faith As Well As Oversight and Risk Management Duties

After *Smith v. Van Gorkom*, Delaware courts severely narrowed oversight and monitoring duties. Following *Caremark*, the court briefly required a "sustained or systematic" failure to monitor.[70] *Stone v. Ritter* limited the scope of the duty to monitor, holding that liability is given only if "(a) the directors utterly failed to implement any reporting or information system or controls *or* (b) having implemented such system or controls,

---

made after making an independent assessment of the information or advice, having regard to the director's knowledge of the corporation and the complexity of the structure and operations of the corporation . . . ."); Mark Byrne, *Do Directors Need Better Statutory Protection when Acting on the Advice of Others?*, 21 AUSTL. J. CORP. L. 238, 253 (2008) (proposing the relaxation of the terms of this provision by means of requiring inquiry only "if the circumstances indicate the need for inquiry").

64. 488 A.2d 858 (Del. 1985).

65. *See* 44 Del. Laws 423 (1943).

66. *Van Gorkom*, 488 A.2d at 875.

67. *Id.* (holding that (a) the CEO's oral presentation did not constitute "reports" within the meaning of Section 141(e) (the current version of this provision includes, though, "information, opinions, reports or statements"); (b) the presentation lacked substance, since the CEO was "basically uninformed as to the essential provisions of the very document about which he was talking"; and (c) the CFO's report did not enjoy the status conferred by Section 141(e), since it was not pertinent as to the subject matter upon which the board is called to act (in fact, it did not purport to be a valuation study)).

68. *Id.* at 877.

69. *Id.* at 875.

70. *See In re* Caremark Int'l, Inc. Derivative Litig., 698 A.2d 959, 963, 971 (Del. Ch. 1996).

[directors] consciously failed to monitor or oversee its operations."[71] The court also required that directors knew that they were not discharging their fiduciary obligations.[72] In interpreting these holdings, subsequent court decisions adopted one of the following approaches.[73] In *Desimore v. Barrows* and *Wood v. Baum*, the courts required facts showing that the board actually *knew*—not *should have known*—that the internal controls of the corporation were inadequate.[74] In *American International Group v. Greenberg*, the court inferred such knowledge from the positions of the directors or officers in the company—which enabled the control of the relevant corporate divisions—as well as from the persistence and the magnitude of the fraudulent conduct.[75] However, in *In re Citigroup, Inc. Shareholder Derivative Litigation*, the court noted that *American International Group v. Greenberg* involved pervasive fraudulent and criminal conduct, as opposed to the failure to recognize the extent of the company's business risk.[76] To be liable for the latter, the court concluded that bad faith must be proven based on the fact that the director knowingly violated a fiduciary duty or demonstrated a conscious disregard for a known duty.[77] Ignoring several red flags indicating deterioration of the subprime mortgage market was insufficient for the duty to monitor to be violated.[78] With regard to the company's failure to disclose exposure to subprime assets, the court rejected demand futility, noting that bad faith would have been proven if plaintiffs demonstrated that directors knew that there were misstatements or omissions in the financial statements.[79]

---

71. *See* Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) (emphasis in original). Furthermore, the court viewed the duty to monitor as a subsidiary element of acting in good faith, while it considered good faith, in turn, as a subsidiary element of the duty of loyalty. *Id.* at 368.

72. *See id.* at 370.

73. *See* Eric J. Pan, *A Board's Duty to Monitor*, 54 N.Y.L. SCH. L. REV. 717, 733 (2009–10).

74. Desimore v. Barrows, 924 A.2d 908, 940 (Del. Ch. 2007) (relating to backdating of stock options); Wood v. Baum, 953 A.2d 136, 139, 141 (Del. 2008) (relating to inadequate accounting and financial-reporting controls).

75. 965 A.2d 763, 795–99 (Del. Ch. 2009) (relating inter alia to improper accounting).

76. 964 A.2d 106, 130 (Del. Ch. 2009) (contrasting the alleged failure to monitor and manage risks Citigroup faced in the context of subprime lending market as well as disclosure failures).

77. *Id.* at 125.

78. *See* Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34 J. CORP. L. 967, 990 (2009) (concluding that claims alleging risk management failure will rarely result in liability).

79. *In re Citigroup*, 964 A.2d at 133–34; *see also* Kevin F. Brady & Francis G.X. Pileggi, *Recent Key Delaware Corporate and Commercial Decisions*, 6 N.Y.U. J. L. & BUS. 421, 429 (2010) (summarizing the court's ruling on the plaintiff's demand futility argument in *In re Citigroup, Inc. Shareholder Derivative Litigation*).

3. Impact on Reliance

The purpose of this review of recent Delaware decisions is to shed light on the interpretation of good faith. Good faith, as noted, is the main pathway to eliminate blind reliance cases under Delaware law.[80] When interpreting "good faith" in Section 141(e), one should not disregard current holdings of Delaware courts relating to this legal concept. In particular, it is fair to speculate that Delaware courts would be unwilling to construe a broad good faith requirement within the reliance framework that would be actually incompatible with its general good faith perception.

Without claiming that the above decisions form a consistent and clear system of rules, the bottom line is that unacceptable blind reliance in Delaware should be limited to cases where directors exhibit bad faith by means of (a) consciously disregarding their duties or (b) demonstrating clearly egregious behavior, such as abdicating their responsibility to make any business decision.[81] At the same time, the court might weigh the magnitude and persistence of the faulty behavior and the director's personal characteristics—mainly the director's experience and position in the company.[82] Therefore, as a rule, "should-have-known" cases do not render reliance unwarranted, as long as the directors act in good faith. Contrary interpretations would be inconsistent with the statute's wording, according to which directors are "fully protected" as long as Section 141(e)'s conditions are met. They would also construe good faith autonomously—that is, regardless of the court's interpretations in other contexts involving bad faith. Therefore, courts will generally not deny Section 141(e) applicability where the director negligently ignores some obvious red flags[83] or otherwise acts in a grossly negligent manner because of the court's (pre-*Caremark*) holdings in *Brehm v. Eisner* and *Ash v. McCall* that reliance is inapplicable where particularized facts show that the issue was material and "so obvious that the board's failure to consider it was grossly negligent regardless of the expert's advice or lack of advice."[84]

---

80. *See supra* Section III.A.

81. *Cf.* Official Comm. of Unsecured Creditors of Integrated Health Servs., Inc. v. Elkins, No. Civ. A. 20228-NC, 2004 WL 1949290 *1, *10 (Del. Ch. Aug. 24, 2004) (interpreting "good faith" in the context of Section 102(b)(7)).

82. *See In re* Emerging Commc'ns, Inc. S'holders Litig., No. Civ. A. 16415, 2004 WL 1305745, at *1, *39–40 (Del. Ch. June 4, 2004).

83. *See id.* at *4 (noting that the directors of an acquiring company ignored various "red flags" including news articles and analysts' reports questioning the financial situation of the company to be acquired). *But see id.* at *9–10 (further noting that the court was satisfied by reliance on experts and the "green flags" they provided and thus, even from the perspective of *Ash v. McCall*, the "so-obvious" exception to reliance should be strictly interpreted).

84. *See* Brehm v. Eisner, 746 A.2d 244, 262 (Del. 2000); Ash v. McCall, No. Civ. A. 17132, 2000 WL 1370341, at *1, *9 (Del. Ch. Sept. 15, 2000).

4. Two Examples

To illustrate this set of rules, this Article considers two real-life examples involving financial statements. The first shows what would *not* occur in Delaware, and the second presents a realistic context of proper reliance under Delaware law.

i. ASIC v. Healey

The following facts took place in Australia, and the circumstances led to the issuance of a well-discussed Federal Court decision entitled *Australian Securities and Investments Commission (ASIC) v. Healey*, which was signed by Justice Middleton.[85] ASIC sued seven directors, six of whom were non-executive, as well as the Chief Financial Officer ("CFO") of the Centro Group over certain errors in the group's financial statements.[86] In particular, about $2 billion (AUD) of current liabilities had been misclassified as non-current liabilities and, in addition, there was a failure to disclose guarantees of short-term liabilities of an associated company of about $1.75 billion (USD) that had been given after the balance date.[87] ASIC claimed that, in failing to notice such a significant error in the statements, defendants breached their statutory duty of care and diligence owed to the group's companies.[88] PricewaterhouseCoopers ("PwC"), a qualified external auditor with complete access to all relevant information, prepared the financial statements.[89] At the same time, the CFO did not warn the directors that there might be irregularities in the statements. The directors, therefore, argued that they reasonably relied on the advice of PwC and of management, adding that they took reasonable steps to ensure that the company had all the necessary procedures and processes in place to prevent such errors.[90] According to Justice Middleton, however, directors (executive and non-executive) retain the ultimate responsibility for financial reporting, and they should recognize the distinction between

85. *Austl. Sec. & Inv. Comm'n v. Healey* [2011] FCA 717 (Austl.), *available at* http://www.austlii.edu.au/au/cases/cth/FCA/2011/717.html; *see, e.g.*, John Lowry, *The Irreducible Core of the Duty of Care, Skill and Diligence of Company Directors:* Australian Securities and Investments Commission v Healey, 75 MOD. L. REV. 249 (2012) (evaluating the impact of the *Australian Securities and Investments Commission v. Healey* decision on the standard of care required for non-executive directors in monitoring the production of financial statements).

86. *Healey*, [2011] FCA 717, at ¶¶ 2–3.

87. *Id.* at ¶ 9.

88. *Id.* at ¶ 8.

89. *Id.* at ¶ 35.

90. David A. Katz, *For Directors, A Wake-Up Call from Down Under*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Oct. 4, 2011, 9:21 AM), http://blogs.law.harvard.edu/corpgov/2011/10/04/for-directors-a-wake-up-call-from-down-under/.

current and non-current liabilities even if they are not experts in accounting.[91] In addition, Justice Middleton described a set of responsibilities of the board with regard to its duty to monitor.[92] Even though he did not cite the reliance provision of Australian corporate law, it appears that he adopted the provision's main requirement: boards need to assess the advice independently; otherwise, the reliance defense does not apply.[93] Finally, in a subsequent decision, Justice Middleton was satisfied by a declaration of contravention signed by the non-executive directors and did not impose further penalties.[94]

One could speculate that this result would not have occurred in Delaware.[95] First and foremost, there was no evidence of bad faith, which under Section 141(e) would render reliance unwarranted. As Justice Middleton admitted, the directors reasonably expected that PwC would provide sound advice, since no " 'red flags' ought to have alerted the directors to deficiencies in the processes or personnel of Centro or its auditors."[96] Justice Middleton's notion that directors *should have known* of the short-term debt and the guarantees is inconsistent with Delaware's interpretation of oversight duties. Assuming that there is no "sustained or systematic" failure to monitor, the *Caremark*-shaped duty to monitor would not be violated. Consequently, Justice Middleton's finding that directors are allowed to rely upon others—except where they know or, by the exercise of ordinary care, *should know* facts that would deny reliance seems to be incompatible with Section 141(e) and Delaware courts' holdings.[97]

---

91. *Healey*, [2011] FCA 717, at ¶ 18 ("[A] director, whatever his or her background, has a duty greater than that of simply representing a particular field of experience or expertise.").

92. *Id.* at ¶ 17 ("[A] director should acquire at least a rudimentary understanding of the business of the corporation and become familiar with the fundamentals of the business in which the corporation is engaged; a director should keep informed about the activities of the corporation; whilst not required to have a detailed awareness of day-to-day activities, a director should monitor the corporate affairs and policies; a director should maintain familiarity with the financial status of the corporation by a regular review and understanding of financial statements; a director, whilst not an auditor, should still have a questioning mind.").

93. *Corporations Act 2001* (Cth) § 189(b) (Austl.); *see also* Byrne, *supra* note 63, at 253.

94. *See Austl. Sec. & Inv. Comm'n v. Healey* (No. 2) [2011] FCA 1003, ¶¶ 188–91 (Austl.) (noting that damage to reputation is sufficient as a general deterrent). The CEO and the CFO, however, incurred a monetary penalty and a temporary disqualification ban, respectively. *Id.*

95. Here, this Article refers only to holdings of the court relating to reliance. The rest of the court's holdings imposing heightened responsibilities on non-executive directors do not correspond to practice in Delaware.

96. *See Healey*, [2011] FCA 717, at ¶ 384.

97. *See id.* at ¶ 167.

ii. Chung v. Nara

The second set of facts is taken from *Chung v. Nara Bancorp*, a 2012 California Court of Appeals decision.[98] The court, applying Delaware law, dealt with a suit filed by Thomas Chung, the ex-chairman of the board of a bank holding company, Nara Bancorp. The suit alleged breach of fiduciary duties by the directors due to the restatement of certain financial statements. It alleged that, in 2002, the Chief Executive Officer ("CEO") prepared a letter stating that he would not withdraw half of the profit share due to him in 2003 and 2004 in exchange for future compensation to avoid falling short of analyst expectations.[99] The 2002 financial statements did not reflect the obligation to the CEO, according to this arrangement.[100] Therefore, in 2005, the audit committee initiated an investigation conducted by a law firm that was assisted by an accounting company.[101] The law firm, the accounting company, and Nara's independent auditor concluded that a restatement of the 2002 financial statements was advisable. Accordingly, the board issued a restatement.[102] Subsequently, within the framework of an arbitration initiated by Nara against the CEO, it was held that there was no need to restate the statements.[103] In 2008, the board decided not to restate (again) the statements and not to sue its advisors. According to the plaintiff, this inaction also constituted a breach of fiduciary duties.[104]

The court noted that both Sections 102(b)(7) and 141(e) are statutory defenses implicating the concept of good faith.[105] Bad faith, in turn, is not established by showing instances of gross negligence, but, according to *Walt Disney*, presupposes more acute forms of misbehavior, such as a conscious disregard for known duties.[106] Since the business judgment rule does not always protect an irrational and grossly negligent decision, the question that arises is whether the two statutory defenses impose a higher hurdle to liability than the business judgment rule. The California court explicitly affirms this to be the case.[107] Accordingly, the court held that "it

98. No. B229826, 2012 Cal. App. Unpub. LEXIS 842, at *1 (Cal. App. Feb. 1, 2012).

99. *Id.* at *2.

100. *Id.* at *3.

101. *Id.*

102. *Id.* at *4.

103. *Id.* at *7.

104. *Id.* at *8.

105. DEL. CODE ANN. tit. 8, §§ 102(b)(7), 141(e).

106. *See In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 67 (Del. 2006); *see also Chung*, 2012 Cal. App. Unpub. LEXIS 842, at *14.

107. *Chung*, 2012 Cal. App. Unpub. LEXIS 842, at *14 ("[A]n irrational and grossly negligent decision may not be protected by the business judgment rule, but it could

is unreasonable to infer that the 2005 Directors consciously disregarded duties or risks when they made their decision to issue the restatement only after hundreds of hours of investigation and only after receiving advice from competent professionals."[108] In other words, the court refused to accept bad faith.

Therefore, the court concluded that Section 141(e) shields directors from liability,[109] since there was no evidence that the directors acted "for a purpose other than advancing the best interests of Nara or [that they] intentionally fail[ed] to act in the face of a known duty to act[.]"[110] It also determined that the directors had not "act[ed] with the intent to violate the law[.]"[111] It was undisputed that the advisors had the "requisite expertise to conduct the investigation," "that they were selected with reasonable care," and that the directors "in fact relied on the recommendation of [the advisors]."[112] In fact, the court referred to the elements of Section 141(e), and, as far as the good faith element is concerned, it adopted the Delaware interpretation.[113]

Finally, with regard to the 2008 directors, the court was satisfied by the defendants' declaration that they "exercised their business judgment in making post arbitration decisions, and that they relied on management and legal counsel to make all legally necessary public disclosures about the arbitration."[114] The same statutory defenses, therefore, protected the directors.[115]

iii. Comparing the Outcomes of the Two Cases

While both cases relate to financial statements, the behavior of the Delaware directors sounds less outrageous. First, the misstatement in the Australia case involved a very substantial sum of money ($2 billion AUD). Second, the Australian directors failed to deal with a very central accounting topic, namely the characterization of liabilities as short term, while the Delaware directors were confronted with a disputed issue. Third, Delaware directors consciously adopted the unanimous view of three independent experts, while the Australian ones just listened to their accountant.

---

very well be protected by an applicable statutory defense.").

108. *Id.* at *21.

109. *Id.* at *22.

110. *Id.* at *15.

111. *Id.*

112. *Id.*

113. *Id.* at *12–15.

114. *Id.* at *23.

115. *Id.* at *25.

On the other hand, for directors, especially for those with no significant financial literacy, there is no meaningful difference between the Australia and the Delaware case: in both cases, they relied on their qualified experts. Since PwC, one of the most well-known accounting companies, failed to spot the irregularity in the statements, the same occurred with non-experts directors. Imposing liability on directors—especially non-executive directors whose duties are mainly supervisory—renders directorship a hazardous job. That is supposedly why Justice Middleton ultimately decided that reputation damages were a sufficient penalty for non-executive directors. He found these directors to be "intelligent, experienced and conscientious people" who undertook their duties honestly, leading him to the conclusion that "they are not people from whom the public must be protected in the future."[116] Justice Middleton, in other words, imposed the most important penalty Delaware directors face, reputation damages.

While the Australia and Delaware statutes differ significantly, they both fail to address all possible issues. Ideally, in assessing reliance, a court should weigh all available information, especially the expertise of the director, the magnitude and nature of the misbehavior, the expert selection process, the efforts to understand the opinion, and then choose a suitable penalty from the ones available in the relevant jurisdiction (declaration of contravention, disqualification, monetary liability, etc.). The good faith requirement in Section 141(e) is too abstract to capture all thinkable sets of facts, while the independent inquiry requirement of the Australian law is too harsh.[117] As the cases examined in this Article show, courts are flexible enough in their effort to reach a fair result.

5. Remaining Uncertainties

The *Smith v. Van Gorkom* holding requiring a reasonable inquiry into the reports submitted by officers (and, inferably, by outside experts) does not correspond to Section 141(e)'s wording and recent judgments relating to good faith.[118] Generally, courts will not condemn "blind reliance"—even if there are signs of grossly negligent behavior—as long as the statutory requirements are met. "Good faith" is interpreted relatively narrowly, according to Delaware court decisions.

One should take note, however, that *Smith v. Van Gorkom* involved an extremely important transaction, namely the acquisition of the company through a cash-out merger. In the context of transactions involving corporate control, the subsequent *Revlon* decision imposed enhanced judicial scrutiny that greatly affected the application of the business

116. *Austl. Sec. & Inv. Comm'n v. Healey* (No. 2), [2011] FCA 1003 ¶ 184 (Austl.).

117. *Corporations Act 2001* pt. 2D.1, div. 1, § 189(b) (Austl.).

118. Smith v. Van Gorkom, 488 A.2d 858, 893 (Del. 1985).

judgment rule in such transactions.[119] The reliance doctrine could not have been left untouched. On the one hand, various decisions, mainly from the 1980's, required that boards actively participate in and oversee the transaction, even if they act according to advisors' opinions.[120] These decisions also questioned the quality of fairness opinions provided by investment banks when their preparation was obviously deficient.[121] On the other hand, there are numerous cases where courts, without citing Section 141(e), treat fairness opinions as a serious indicator that directors properly acted in approving the relevant transaction.[122] Consequently, fairness opinions are an element supporting that the director was not "grossly negligent" in informing himself, and therefore that business judgment presumption applies. Section 141(e) as a defense is usually not dealt with or is seen as inapplicable in gross negligence cases.[123] Without asserting that Section 141(e) is the appropriate tool to deal with the complexities of fairness opinions, it is clear that there are a lot of uncertainties, which this Article will not address.

B. Should the Advice Be Written and Formally Presented?

The court in *Smith v. Van Gorkom* was not satisfied by an oral presentation; it required a written report to fulfill Section 141(e)'s dictate.[124] Since the current version of this provision includes

119. Revlon, Inc. v. MacAndrews & Forbes Holdings, Inc., 506 A.2d 173, 184–85 (Del. 1986).

120. *See* Mills Acquisition Co. v. MacMillan, Inc., 559 A.2d 1261, 1281 (Del. 1988) (holding that "in a matter as significant as the sale of corporate control," directors cannot avoid an "active and direct duty of oversight" simply by conditioning the transaction on the outsider's opinion); *see also In re* Healthco Int'l, Inc., 208 B.R. 288, 305–06 (Bankr. D. Mass. 1997); Cede & Co. v. Technicolor, 634 A.2d 345, 369 (Del. 1993); William T. Allen, Jack B. Jacobs & Leo E. Strine, *Function Over Form: A Reassessment of Standards of Review in Delaware Corporation Law*, 56 BUS. LAW. 1287, 1300 (2001) ("[O]utside directors who had approved an arm's-length-negotiated sale of their company to an unrelated third party, in reliance upon the advice of independent counsel and investment bankers, were found to be . . . grossly negligent for not having "shopped" the company before agreeing to the sale . . . .").

121. *See* Joseph v. Shell Oil Co., 482 A.2d 335, 344 (Del. Ch. 1984) (criticizing opinions that were prepared in a very short period of time); *accord* Weinberger v. UOP, Inc., 457 A.2d 701, 712 (Del. 1983).

122. *See, e.g.*, Steven M. Davidoff, *Fairness Opinions*, 55 AM. U. L. REV. 1557, 1599 n.221 (2006).

123. *See, e.g.*, *Cede & Co.*, 634 A.2d at 366; *see also* Crescent/Mach I Partners, L.P. v. Turner, 846 A.2d 963, 985 (Del. Ch. 2000) ("Section 141(e) of Delaware's corporation law provides that directors are protected from a breach of the duty of care 'when the directors reasonably believe the information upon which they rely has been presented by an expert 'selected with reasonable care' and is within that person's 'professional or expert competence.' ").

124. 488 A.2d 858, 884 (Del. 1985).

"information, opinions, reports or statements," one could hardly argue that oral presentations are unacceptable only because of their oral nature.[125] Of course, directors might prefer written reports, since judicial review will be easier.[126]

Similarly, there is no need for a formal presentation to the board of directors.[127] The wording of Section 141(e) ("presented to the corporation") does not exclude written presentations but requires some form of presentation. If the director fails to attend oral presentations or does not read the reports, it could be argued that there was no *stricto sensu* reliance—that is, an act *based on* the advice.[128]

C. Waste or Fraud

Decisions of the board "so unconscionable as to constitute waste or fraud" are not excused by reliance.[129] There is no need to expand Section 141(e), since bad faith covers both concepts. With regard to fraud, that is obvious. In considering waste, the Delaware Supreme Court has held that waste constitutes bad faith.[130] It should be noted, however, that waste will rarely be found. If "there is *any substantial* consideration received by the

---

125. *See* Uebler, *supra* note 24, at 1037–38 ("[P]urpose of the 1987 amendment was 'to clarify that directors may rely in good faith upon . . . written or oral advice or opinions of any professionals and experts . . . .' ").

126. *See* Carlton Invs. v. TLC Beatrice Int'l Holdings, No. Civ. A. 13950, 1997 Del. Ch. LEXIS 86, at *54 (Del. Ch. May 30, 1997) ("[A]lthough a written legal opinion is preferable from the standpoint of a court engaged in a post facto review of a board's decision, whether an opinion is oral or in writing is of no consequence to the board at the time of its decision."); *see also* Hawes & Sherrard, *supra* note 16, at 33.

127. *See In re* Walt Disney Co. Derivative Litig., 907 A.2d 693, 769 n.550, *aff'd*, 906 A.2d 27 (Del. 2006) ("Nor is it necessary for an expert to make a formal presentation at the committee meeting in order for the board to rely on that expert's analysis, although that certainly would have been the better course of action.").

128. *See In re* Healthco Int'l, Inc., 208 B.R. 288, 307 (Bankr. D. Mass. 1997) ("The defendants say they relied on the solvency opinions of Valuation Research Corporation. But they never saw those opinions before approving the transaction, so the opinions can hardly constitute 'reports' of an expert the directors were entitled to rely upon under section 141(e) of Delaware's corporation law."); MODEL. BUS. CORP. ACT ANN., § 8.30(e), at 8-202 (2011 Revision) ("Reliance . . . is permitted only if the director has read the information, opinion, report or statement in question, or was present at a meeting at which it was orally presented, or took other steps to become generally familiar with it."). However, as this Article notes previously, a director who read the report but failed to familiarize himself with it loses the reliance defense only in bad-faith cases.

129. *See* Brehm v. Eisner, 746 A.2d 244, 262 (Del. 2000).

130. *See In re* Citigroup, Inc. S'holder Derivative Litig., 964 A.2d 106, 136 (Del. Ch. 2009) (quoting White v. Panic, 783 A.2d 543, 554 n.36 (Del. 2001)) ("To prevail on a waste claim . . . the plaintiff must overcome the general presumption of good faith by showing that the board's decision was so egregious or irrational that it could not have been based on a valid assessment of the corporation's best interests.").

corporation, and if there is a *good faith judgment* that in the circumstances the transaction is worthwhile, there should be no finding of waste," and Section 141(e) will be applicable.[131]

D. Full Disclosure

Even before the enactment of Section 141(e) and MBCA Section 8.30(e) in their current versions, courts unanimously held that the reliance defense is not available to directors who fail to disclose all relevant facts to their advisor.[132] For example, factual distortions calculated to result in favorable advice clearly violate good faith principles and thus exclude the use of the defense.[133] Similarly, withholding from advisors facts that the director thinks are relevant can be a "clear indication of bad faith."[134] For example, directors of an oil company should disclose material, non-public information on the value of probable oil reserves to an investment banker; otherwise, the fairness opinion is deficient.[135] Due to Section 141(e)'s wording, it is unclear whether an honest, but grossly negligent failure to disclose some facts taints the defense. This would be the case when the director, due to the complexity of the issues involved, fails to recognize which facts are relevant. If this failure is not attributed to negligence, the omission would be "innocent."[136] If the failure is attributed to gross negligence, but the director acts in good faith, the result of a strict interpretation of Section 141(e) would not exclude reliance. The exercise of the advisor's duty, though, to ask appropriate questions to receive the necessary information might prevent some of these cases of gross negligence.[137]

---

131. Lewis v. Vogelstein, 699 A.2d 327, 336 (Del. Ch. 1997) (emphasis in original).

132. Hawes & Sherrard, *supra* note 16, at 29 (regarding disclosure to attorneys).

133. Comment, *Reliance on Advice of Counsel*, 70 YALE L.J. 978, 989 (1961).

134. *Id.* at 981; *see also* Uebler, *supra* note 24, at 1044 ("[A]nything less than full disclosure by the directors to the expert of all material facts related to the subject of the expert advice might evidence bad faith.").

135. Joseph v. Shell Oil Co., 482 A.2d 335, 341 (Del. Ch. 1984).

136. Hawes & Sherrard, *supra* note 16, at 29 (noting that requiring negligence is consistent with the general structure of the defense, since, for example, directors are shielded if they reasonably believe in the advisor's competence).

137. *Id.* at 29 n.116; Longstreth, *supra* note 39, at 1192. For example, a bankruptcy court examining a fraudulent transfer was not satisfied by reliance on a solvency opinion issued by a consulting firm where this firm (a) would receive the larger part of its payment only if it issued a favorable opinion and (b) relied on the outdated projections provided by the management—as well as on management's "downside" models—without making an independent inquiry. *In re* TOUSA, Inc., 422 B.R. 783, 839–40 (Bankr. S.D. Fla. 2009), *rev'd, In re* TOUSA, Inc., 444 B.R. 613 (S.D. Fla. 2011), *aff'd in part, rev'd in part* 680 F.3d 1298 (11th Cir. 2012). *But see* Jeffrey Rothschild, *Court Rulings on Solvency and Fairness Opinions Help to Define Liability for Financial Advisors*, MCDERMOTT WILL & EMERY (Feb. 2010),

A variation of the lack of disclosure problem arises when CEOs entrusted with the transmission of information to the expert manipulate the information to prevent undesirable reports.[138] Clearly, Section 141(e) does not deal with that problem in its entirety. As noted previously, there is no prejudice against experts selected by management.[139] Nevertheless, since boards are required to demonstrate reasonable care when selecting advisors, they should not allow conflicted managers to select experts and control the flow of information between the corporation and the experts. In the presence of instances justifying a particular interest of managers in the transaction (when, for example, they are to receive a large bonus or benefit upon the consummation of a deal), directors should prevent them from hiring a "friendly" advisor, or at least ensure that the advisor receives all necessary information, in order to be able to enjoy the benefits of Section 141(e). In the absence of such circumstances, reliance is considered warranted.[140] Therefore, Section 141(e) fails to address the incentives of managers, who, without being conflicted, try to manipulate the information experts receive. Managers attempting to escape the board's oversight by relying on expert opinions will usually be ineffective.[141]

E. Causal Nexus

Opinions that are not pertinent to the decision to be made[142] are not covered by Section 141(e) because there is no *stricto sensu* "reliance." Generally, for liability to be precluded there must be a causal nexus between the challenged aspect of the transaction and the advice.[143]

Sometimes, causal nexus theories may benefit the recipient of the advice,

---

http://www.mwe.com/info/pubs/CRI_3%201_Rothschild.pdf (noting that in various cases courts were unwilling to hold financial advisors liable for fairness opinions, when limitation on liability is explicitly stated in engagement letters).

138. *See* Nina Walton, *Delegated Monitoring: When Can Boards Rely on Outside Experts?*, 14 AM. L. ECON. REV. 271, 277, 294 (2012) (concluding that, to eliminate the incentives of managers to manipulate experts, boards should ask for joint recommendations signed by both managers and experts).

139. *See supra* Section II.D.

140. *Cf.* Cox, *supra* note 43, at 1090 ("Though there is always the fear that managerial self-interest will corrupt the information that reaches the board, absent notice to the contrary, boards are entitled to rely upon reports prepared by managers and their stewards unless the directors are aware of circumstances that make such reliance unreasonable.").

141. *See* Walton, *supra* note 138, at 275, 299; *see also* Valeant Pharms. Int'l v. Jerney, 921 A.2d 732, 751 (Del. Ch. 2007).

142. *See* Smith v. Van Gorkom, 488 A.2d 858, 875 (Del. 1985); *see also Valeant Pharms. Int'l*, 921 A.2d at 751.

143. Uebler, *supra* note 24, at 1045–46 ("There may be no causal nexus, however, where, with respect to a fairness opinion by a financial expert, the unfairness of the transaction relates to process (e.g., timing or structure) and not to price.").

for example when there is failure to disclose all facts to the expert, but the challenged aspect of the transaction does not relate to the undisclosed facts.

F. Contractual Relationship

A direct contractual relationship between the company and the advisor is not required,[144] provided, of course, that the advisor is selected with reasonable care and directors act in good faith.[145] The board may equally rely on the accounting company engaged by the company's law firm,[146] on the legal advisor of the underwriter,[147] or on the expert engaged by another company participating in a common project or joint venture. However, according to Section 141(e), there has to be some kind of presentation to the board, such as a written report by the expert. Furthermore, it is questionable whether a total stranger can present to the corporation information, opinions, reports, or statements within the meaning of Section 141(e). Consequently, published articles of experts or published ratings cannot be used to invoke a Section 141(e) defense.[148] Thus, a board approving investments in highly rated investment products may allege that it was not grossly negligent in informing itself, but it cannot invoke Section 141(e).

CONCLUSION

In all walks of corporate life—from creation to expansion and from restructuring to demolition—experts are available to advise all players—directors, managers, shareholders, financiers, etc. Section 141(e) does not regulate the role of experts, but only the conditions under which reliance on them is statutorily protected. This Section, specifically the part relating to experts, does not come into play as often as one would imagine. First, it applies only to directors. Second, when it comes to liability, directors are shielded by various alternative mechanisms, ranging from the business judgment presumption and the Section 102(b)(7) exculpatory clause to indemnification and D&O insurance provisions.[149] At the same time, when Section 102(b)(7) is inapplicable due to the bad faith of the director,

144. *See* MODEL BUS. CORP. ACT § 8.30(f)(2) ("persons retained by the corporation"). This wording invites contrary interpretations.

145. *See supra* Section II.B, II.D.

146. Chung v. Nara Bancorp, No. B229826, 2012 Cal. App. Unpub. LEXIS 842, at *3 (Cal. Ct. App. Feb. 1, 2012).

147. Hawes & Sherrard, *supra* note 16, at 26–27.

148. *Cf.* Lyman P.Q. Johnson, *The Audit Committee's Ethical and Legal Responsibilities: The State Law Perspective*, 47 S. TEX. L. REV. 27, 31 (2005) (noting that reliance on a CFO's views as reported in an interview with a newspaper is not appropriate).

149. DEL. CODE ANN. tit. 8, §§ 102(b)(7), 145(a), 145(g).

Section 141(e) will not usually be applicable either. Therefore, Section 141(e) would be useful for the director, for instance, in the event of conflicted transactions or when there is gross negligence in the information gathering process and no Section 102(b)(7) protection is in place.

In such cases, unfortunately, the holdings of Delaware courts are not completely consistent. One would expect that the elements of Section 141(e) would provide satisfactory (and exclusive) guidance to the courts, but the courts often are either indecisive with regard to the interpretation of the good faith element, add extra elements to the rule, or do not cite Section 141(e) at all. While, for example, a court decision inferred from the particular qualifications of a director that he "should have known," another decision stated that even directors who are experts are fully protected under Section 141(e).[150] Most importantly, although the provision does not require directors to conduct an independent inquiry, Delaware courts, especially in merger and conflicted transactions, (a) require boards to be active,[151] (b) take into account facts the directors did not know[152] or could not have known, (c) consider reliance inapplicable when "the subject matter that was material and reasonably available was so obvious that the board's failure to consider it was grossly negligent regardless of the expert's advice or lack of advice,"[153] or (d) consider reliance as "a pertinent factor in evaluating whether corporate directors have met a standard of fairness in their dealings with respect to corporate powers."[154] While not resolving all uncertainties, this Article concludes that, according to the wording of Section 141(e), and taking into account *Caremark*,[155] Delaware courts are expected to interpret this provision as the *Chung v. Nara* court did.[156] Accordingly, Section 141(e) is construed as a "standalone" defense, which can shield grossly negligent directors even when they are not protected by the business judgment presumption.

Had the Wisconsin schools been a Delaware corporation, its directors would probably have been fully protected by both the business judgment presumption and the reliance provision. Of course, in Delaware there are alternative mechanisms, most notably reputational mechanisms that could

150. *See In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106, 135 (Del. Ch. 2009).

151. *See supra* Section III.A.5.

152. *See* Valeant Pharms. Int'l v. Jerney, 921 A.2d 732, 751 (Del. Ch. 2007) (admitting that the board probably did not know that the advisor had already issued an opinion favoring the award of bonuses).

153. Brehm v. Eisner, 746 A.2d 244, 262 (Del. 2000).

154. Cinerama, Inc. v. Technicolor, Inc., 663 A.2d 1134, 1142 (Del. Ch. 1994), *aff'd*, 663 A.2d 1156 (Del. 1995); *see also Valeant Pharms. Int'l*, 921 A.2d at 751.

155. *See supra* Section III.A.2.

156. *See supra* Section III.A.4.ii.

have affected their behavior. "In Delaware," as two Delaware attorneys put it, "the answer is not to expand their personal liability."[157]

157. *See generally* Dominick T. Gattuso & Vernon R. Proctor, *Reining in Directors and Officers in Corporate America*, 19 BUS. L. TODAY 1 (Jan./Feb. 2010). However, even from a reputation perspective, this does not mean that there is no need for more predictable rules. For directors, even having to participate in a trial might (at least temporarily) damage their reputation.

* * *

COMMENTS

PETITIONING FOR CASH: HOW DOMESTIC INDUSTRIES EXPLOIT ANTIDUMPING PROCEDURES AND ANTITRUST EXCEPTIONS TO FORCE THEIR FOREIGN COMPETITORS INTO LUCRATIVE SETTLEMENT AGREEMENTS

DANIEL FULLERTON*

The United States' international trade laws strictly enforce antidumping ("AD") rules, and its antitrust laws effectively oversee private settlement agreements. However, these two distinct, yet related, areas of law both fail to adequately address the legality of private post-order settlement agreements that occur in the shadows of the AD process. This Comment investigates the legality of such settlements and reveals how domestic firms are exploiting the overlap between AD and antitrust laws so as to circumvent both. Being fully aware that AD administrative reviews create costly uncertainty for foreign firms, domestic firms exploit this uncertainty and pressure their foreign competitors into agreeing to lucrative cash settlement agreements. Though these settlements frustrate the object and purpose of AD laws by incentivizing unfairly priced imports, the settlements sidestep existing AD laws and are not prohibited. Normally, such collusive efforts to disrupt trade would create immediate antitrust

* Staff member, *American University Business Law Review*, Volume 2; J.D. Candidate, *American University, Washington College of Law*, 2014; B.A. Government & Economics, *The College of William & Mary*, 2011. Many thanks to my editors, Jamie Hennelly, Jodie Bensman, and Amit Raviv, and the entire staff of the *American University Business Law Review* for all of their edits and advice on this piece. I would like to especially thank Clara for supporting and encouraging me throughout the writing process and for always being my most critical and constructive editor. Finally, a special thank you to my family for their constant support and for always encouraging me to challenge myself.

liability, but the Noerr-Pennington Doctrine, with its First Amendment foundations, immunizes domestic firms from liability. This Comment takes a closer look at the legal implication of these settlement agreements in both antitrust and international trade contexts. It then suggests ways to restore the functional effectiveness of AD laws.

TABLE OF CONTENTS

INTRODUCTION

Within the United States' international trade framework, domestic industries can exploit U.S. antidumping ("AD") laws to seek private monetary gain, restrain trade, and harm competition.[1] Though this practice is not new, it operated almost entirely in secrecy until the International Trade Commission ("ITC") recognized its existence during a recent investigation.[2] The discovery of this practice even caused one ITC Commissioner to proclaim, "I cannot figure out for the life of me how [this practice is] actually legal."[3] The ITC, however, lacked the jurisdiction to

1. *See* Kenneth J. Pierce & Robert E. DeFrancesco, *The New Big Thing in Trade Law: Post-Order Antidumping and Countervailing Duty Settlements*, METRO. CORPORATE COUNSEL. (Sept. 1, 2006), http://www.metrocorpcounsel.com/pdf/2006/September/05.pdf (describing a "new" international trade practice).

2. *See* Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203, at 16 (Dec. 2010) (Review) [hereinafter Chinese Furniture] (acknowledging the existence of this practice); James R. Hagerty, *Cash Softens a Trade Blow*, WALL ST. J. (Feb. 15, 2011), http://online.wsj.com/article/SB10001424052748704081604576144401022132530.html.

3. Transcript of Record at 86, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Oct. 5, 2010) (Review) [hereinafter Transcript] (statement of Comm'r Lane).

address the legality of this practice.[4]

The United States maintains a system of trade laws to facilitate international commerce and protect domestic industries from unfair competition.[5] Specifically, AD laws strive to overcome the harmful effects of dumping, a practice that occurs when a foreign firm sells goods in the U.S. market at unfairly low prices.[6] To prevent these artificially low-priced goods from affording an unfair competitive advantage to foreign firms at the expense of domestic industries, the U.S. government assigns AD duties to foreign goods that are dumped in the U.S. market.[7]

The duty rates, however, are non-permanent and are subject to annual administrative reviews.[8] These reviews create costly uncertainty for foreign firms, and domestic industries are quick to exploit this uncertainty by pressuring foreign firms into lucrative settlement agreements.[9] Under these agreements, those foreign producers subjected to the AD order ("subject foreign producers") make cash payments to domestic producers, who then withdraw the petitions for administrative reviews, allowing foreign producers to avoid the costly review process.[10]

---

4. *See* Chinese Furniture, *supra* note 2, at 16–17 (asserting that the ITC need not consider the ramifications of such settlement agreements); Simon Lester, *More on Anti-Dumping Payments*, INT'L ECON. L. & POL'Y BLOG (Feb. 21, 2011, 8:37 PM), http://worldtradelaw.typepad.com/ielpblog/2011/02/more-anti-dumping-payments.html (explaining that both the ITC and the Department of Commerce lack jurisdiction over the related antitrust issues).

5. *See* Sungjoon Cho, *Anticompetitive Trade Remedies: How Antidumping Measures Obstruct Market Competition*, 87 N.C. L. REV. 357, 364–68 (2009) (detailing the history and purpose of the U.S. trade laws and arguing that the U.S. AD regime has a pervasive protectionist nature).

6. 19 U.S.C. § 1677(34) (2006); *see* Maurizio Zanardi, *Antidumping Law as a Collusive Device*, 37 CAN. J. OF ECON. 95, 96 (2004) (noting that dumping determinations account for product quantity, quality, and sale circumstances).

7. Marion B. Schnerre, *Antidumping, A Choice Between Unilateral Duties or Negotiation of a Suspension Agreement*, 4 IND. INT'L & COMP. L. REV. 497, 497–98 (1994); *see* STAFF OF H. COMM. ON WAYS AND MEANS, 111TH CONG., OVERVIEW AND COMPILATION OF U.S. TRADE STATUTES 108 (Comm. Print 2010) (describing how AD duties are designed to curtail the effects of international price discrimination); Cho, *supra* note 5, at 370–73 (acknowledging that AD remedies are intended to stop predatory pricing schemes, but pointing to flaws in the rationale behind AD laws).

8. *See* Patrick F. J. Macrory, *Administration of the U.S. Antidumping Law by the Department of Commerce*, 722 PLI/COMM 9, 27–28 (1995) (explaining that original duty rates and final AD liability are subject to change if the Department of Commerce conducts an administrative review of an AD order).

9. *See* HARVEY KAYE & CHRISTOPHER A. DUNN, INTERNATIONAL TRADE PRACTICE § 31:4 (2011) (articulating how firms weigh the costs of uncertainty against their duty rates and final AD liability); Cho, *supra* note 5, at 388 (examining how duty rate uncertainty increases transaction costs for foreign firms).

10. *See* KAYE & DUNN, *supra* note 9 (describing settlements as "attractive options"

These collusive settlement agreements raise important antitrust concerns because they involve private price and quantity agreements that actively restrain commerce, as well as efforts to use government processes for improper purposes.[11] However, due to retrospective AD procedures and First Amendment exceptions to antitrust rules, these settlements are likely permissible under both AD and antitrust laws.[12] Thus, though the ITC may be "very troubled by [such] settlement agreement[s],"[13] an unlikely intersection of international trade and antitrust laws allows domestic industries to circumvent both sets of laws and thus immunize themselves from any actionable liability.

This Comment addresses whether these private post-order settlement agreements are, in fact, legal under existing AD and antitrust frameworks and, if they are legal, how U.S. laws can adapt to account for these settlements. Section II of this Comment discusses the history, purpose, and function of U.S. AD laws. Then, it examines how the administrative review process gives rise to private settlement agreements. Section III analyzes whether these settlements are legal under U.S. antitrust laws and how these settlements frustrate the object and purpose of AD laws. Finally, Section IV recommends ways to adapt U.S. trade laws to account for these settlement agreements. This Comment employs a recent ITC case ("Chinese furniture case")[14] as an example of how post-order AD settlement agreements operate.

I. AD LAWS EVOLVED TO PRODUCE EFFECTIVE MEANS OF PROTECTING DOMESTIC FIRMS FROM UNFAIR IMPORTS, AND THESE LAWS ARE CLOSELY TIED TO ANTITRUST CONCERNS

This Section begins by exploring the history and purpose of AD laws and how they grew in both scope and effectiveness over the last century to build today's complex trade law regime.[15] In particular, this Section

for foreign and domestic firms); Zanardi, *supra* note 6, at 96 (describing how domestic producers "threaten and induce" foreign producers into agreeing to settle).

11. *See* KAYE & DUNN, *supra* note 9 (observing that private pricing agreements can themselves be considered conspiracies in restraint of trade); Terry Calvani & Randolph W. Tritell, *Invocation of United States import relief laws as an antitrust violation*, 31 ANTITRUST BULL. 527, 548 (1986) (arguing that the abuse of import relief mechanisms violates the spirit of the Sherman Act); Schnerre, *supra* note 7, at 498 (outlining the purposes of AD legislation).

12. *See infra* Section II.

13. Transcript, *supra* note 3, at 86 (statement of Comm'r Lane).

14. Chinese Furniture, *supra* note 2.

15. *See* JOHN H. JACKSON, WILLIAM J. DAVEY & ALAN O. SYKES, JR., LEGAL PROBLEMS OF INTERNATIONAL ECONOMIC RELATIONS 763 (Jesse H. Choper et al. eds., 5th ed. 2008) (noting the complex and formalized nature of modern AD rules and

focuses on the AD administrative review process and its retrospective method of determining final AD duty liability. Then, this Section turns to a discussion of antitrust laws and how their regulation of private settlement agreements creates an important juncture of AD and antitrust concerns. Additionally, this Section introduces the Chinese furniture case as an example to describe AD procedures.

A. The Evolving History, Purpose, and Function of AD Laws Created an Effective System of AD Enforcement

Congress first contemplated "dumping" in the Antidumping Act of 1916 ("1916 Act"), which allowed domestic firms to bring suits against foreign firms dumping goods in the U.S. market at less than fair value ("LTFV").[16] The elements of the 1916 statute, however, were difficult to satisfy, and Congress introduced new AD legislation in 1921.[17] Though AD mechanisms continued to strengthen, they remained largely unused until the 1970s.[18]

1. The Trade Agreements Act of 1979 Established the Modern International Trade Law System

Congress ushered in a new era of AD policy with the Trade Agreements Act of 1979 ("1979 Act"), which repealed the 1921 Antidumping Act.[19] Since the implementation of the 1979 Act, the Department of Commerce ("Commerce") and the ITC share the responsibility of investigating and enforcing U.S. AD laws; Commerce determines whether dumping occurred, and the ITC determines whether the dumping caused a domestic industry to suffer a material injury.[20] Today, American industries use AD laws more than any other import relief mechanism.[21]

---

procedures).

16. *See* U.S. INT'L TRADE COMM'N, ANTIDUMPING AND COUNTERVAILING DUTY HANDBOOK IV-3 (13th ed. 2008) (recognizing that domestic firms could seek damages against foreign firms in federal court under the 1916 Act).

17. *See id.* (suggesting that the intent requirements of the 1916 Act were especially difficult to demonstrate).

18. Macrory, *supra* note 8, at 15.

19. *See* U.S. INT'L TRADE COMM'N, *supra* note 16, at IV-4 (describing the 1979 Act as a codification of the GATT Antidumping Code); Macrory, *supra* note 8, at 15 (noting that the 1970s brought both procedural and substantive changes to U.S. AD laws).

20. JACKSON, DAVEY & SYKES, *supra* note 15, at 763–64; *see* U.S. INT'L TRADE COMM'N, *supra* note 16, at IV-4 (explaining that Commerce took over its antidumping administration role from the Department of the Treasury).

21. *See* Macrory, *supra* note 8, at 15 (noting that AD duties, together with countervailing duties, are the most commonly used import relief mechanism).

2. The Byrd Amendment Added Cash to the AD Equation

The Byrd Amendment, or Continued Dumping and Subsidy Offset Act, changed AD laws so that the cash from foreign firms' duty payments went directly to the pockets of domestic firms, instead of being paid into the federal treasury.[22] Thus, "domestic interested parties"[23] had a new reason to bring AD investigations: direct cash payments.[24] Congress, however, repealed the Byrd Amendment, effective October 1, 2007, leaving domestic industries with a "whetted appetite for cash" and contributing to the recent influx in cash settlement agreements.[25]

3. AD Laws Are Built Around the Important Purpose of Limiting the Harmful Effects of Unfair Imports

AD laws strive to maintain fair competition by ensuring foreign goods are not sold at unfairly low prices in the U.S. market.[26] If goods enter the United States at unfairly low prices, foreign firms could drive domestic firms out of the market and create barriers to keep them from reentering the market.[27] Foreign firms could then raise prices well beyond previous market rates, and no domestic competition would exist to quell skyrocketing prices.[28] By providing only administrative remedies, AD laws are not designed to incentivize action by domestic firms seeking direct duty payments; rather, the incentive is supposed to be protection from unfair trading practices.[29]

---

22. *See* Pierce & DeFrancesco, *supra* note 1 (contending that the Byrd Amendment altered trade litigation by changing the incentives associated with bringing AD investigations).

23. 19 U.S.C. § 1677(4)(A) ("[P]roducers as a whole of a domestic like product, or those producers whose collective output of a domestic like product constitutes a major proportion of the total domestic production of the product.").

24. *Id.*

25. *See id.* (arguing that the Byrd Amendment, and its subsequent repeal, was a primary cause of the increasing prevalence of settlement agreements). *But see* JACKSON, DAVEY & SYKES, *supra* note 15, at 812 (questioning the Byrd Amendment's association with private settlement agreements).

26. *See* Schnerre, *supra* note 7, at 497–98 (explaining that AD laws pursue a "level playing field" for international trade).

27. *See* JACKSON, DAVEY & SYKES, *supra* note 15, at 756–63 (providing examples of how the AD process is supposed to function and thus further the underlying policies of AD laws).

28. *See* Schnerre, *supra* note 7, at 497 (identifying the threat of a foreign country gaining an unfair advantage in the domestic market as the primary incentive for domestic industries to initiate AD cases).

29. *Cf. id.* at 517 (explaining that AD laws no longer afford monetary damages for domestic producers but instead incentivize domestic action by eliminating unfair competition).

B. The AD Process Operates Through a System of Petitions, Investigations, Duties, and Reviews

Under U.S. trade law, "dumping" occurs when a foreign firm sells a good in the U.S. market at LTFV.[30] Together, Commerce and the ITC determine whether dumping occurred and whether the dumping materially injured domestic industries.[31] If both decisions are affirmative, Commerce imposes AD duties on all imports from the subject country being unfairly dumped in the U.S. market ("subject imports").[32]

When domestic interested parties believe foreign firms from a specific country are dumping goods in the U.S. market, the domestic interested parties can file AD petitions with Commerce and the ITC.[33] Commerce will issue an affirmative determination and calculate AD duty margins if it finds that subject imports enter the U.S. market at LTFV.[34] Then, the ITC determines whether subject imports cause, or are likely to cause, material injury to a domestic industry.[35] If both Commerce and the ITC reach affirmative final determinations, Commerce assigns AD duties to all subject imports from the subject country.[36] The initial duty rates, however, are not permanent, and domestic interested parties can petition to have them retroactively changed to reflect the actual dumping margins.[37]

Generally, U.S. AD law provides two primary methods for "settling" an AD duty case during the initial investigation process: (1) a suspension agreement, or (2) a withdrawal of the domestic interested party's petition.[38] For suspension agreements, Commerce will stop an investigation so long as

---

30. 19 U.S.C. § 1677(34). *See* Zanardi, *supra* note 6, at 96 (describing dumping as selling a product for cheaper in its own domestic market than the amount for which it is sold in a foreign market); STAFF OF H. COMM. ON WAYS AND MEANS, *supra* note 7, at 108–11 (stating that the LTFV determination involves a comparison of a foreign good's "normal value" and its "export price" and describing how those values are calculated).

31. *See, e.g.*, JACKSON, DAVEY & SYKES, *supra* note 15, at 763–64.

32. *See* Zanardi, *supra* note 6, at 96 (noting AD orders require affirmative final determinations by both Commerce and the ITC).

33. U.S. INT'L TRADE COMM'N, *supra* note 16, at II-4.

34. Macrory, *supra* note 8, at 21.

35. *Id.* at 23.

36. INT'L TRADE ADMIN., IMPORT ADMINISTRATION ANTIDUMPING MANUAL, ch. 1, subdiv. (IV)(A)(3) (last updated Oct. 13, 2009). To satisfy duties imposed by Commerce, cash deposits, not bonds, must accompany all subject imports and must be assessed at the estimated dumping margin. *See* Macrory, *supra* note 8, at 16, 23.

37. *See* JACKSON, DAVEY & SYKES, *supra* note 15, at 766–67 (describing initial duties as mere provisional estimations that can be later changed through annual administrative reviews).

38. Macrory, *supra* note 8, at 24–26.

"substantially all" foreign producers of the subject imports agree to remove the dumped goods' harmful effects.[39] Commerce's approval of a suspension agreement is also contingent upon Commerce's determination that a cessation of the investigation is in the public interest.[40]

Unlike suspension agreements, the cessation of AD investigations via a withdrawal of a petition requires the domestic producers' consent.[41] A petitioner can stop an investigation by withdrawing an AD petition at any point before Commerce's final determination.[42] However, as with suspension agreements, the ultimate cessation of the investigation depends upon Commerce's determination that ending the investigation is in the public interest.[43]

Moreover, an AD duty order can still be removed after it is put in place.[44] Both Commerce and the ITC must conduct reviews of AD orders every five years after the publication of an AD order, and Commerce must revoke an AD order if the agencies find that the order's termination would not lead to a likely continuation or recurrence of dumping or material injury.[45]

C. *By Request, Commerce Can Reevaluate Final AD Duty Liability Through Administrative Reviews*

The margin rates assigned under original AD duty orders are non-permanent estimates.[46] If domestic interested parties want the dumping margins and associated import duties to be retroactively adjusted, they can

39. *See* KAYE & DUNN, *supra* note 9, § 27:3 (explaining that suspension agreements typically require foreign producers to either raise their prices or reduce their import volume); Macrory, *supra* note 8, at 24–25 (detailing a step-by-step process for AD suspension agreements).

40. 19 U.S.C. § 1673c(d)(1).

41. Macrory, *supra* note 8, at 24.

42. *Id.* at 25.

43. *Id.* at 24–25.

44. *See id.* at 22, 24, 30–31 (providing several examples for how an AD order can be removed or revoked).

45. 19 U.S.C. § 1675(c); *see* Macrory, *supra* note 8, at 30–31 (outlining Commerce and the ITC's decision-making process as part of the "sunset review" process); *see also Five-Year ("Sunset") Review Status*, U.S. INT'L TRADE COMM'N (May 31, 2010), http://info.usitc.gov/oinv/sunset.nsf/0a915ada53e192cd8525661a0073de7d/a161c6791613f35b852567750054a793/$FILE/May%2031%202010%20Sunstatus.pdf (detailing Commerce and the ITC's revocation rate under sunset reviews and revealing that many more dumping orders are maintained than are revoked).

46. *See* Macrory, *supra* note 8 (explaining that because original margin rates are non-permanent, foreign firms' duty payments do not necessarily represent their final liability).

petition Commerce for an annual administrative review of the duty rates.[47] Under such a review, Commerce examines the actual import data from the previous year to determine whether the original cash deposit rate was higher or lower than the actual dumping margin.[48] If there are too many foreign firms to review individually, Commerce uses a sampling technique to gather trade data from selected firms and uses that data to generate a nationwide AD duty rate for those firms not investigated individually.[49]

After an administrative review, U.S. Customs and Border Protection ("Customs") provides subject foreign producers with a refund if their initial deposits were too high.[50] Alternatively, if the initial deposits were too low, Customs collects the difference.[51] From then on, cash deposits assessed at the new duty rates must accompany all subject imports.[52]

Requests for administrative reviews occur in a majority of AD cases.[53] However, if Commerce receives no requests for an administrative review, the original estimated AD margins remain, and all subject foreign producers continue to pay their original duty rates.[54] Similarly, a domestic producer's timely withdrawal of a petition for administrative review stops the review process, leaving the original duty rates in place.[55]

Importantly, domestic interested parties can choose which foreign producers are included in a petition for administrative review, causing Commerce to treat foreign producers differently during an administrative review.[56] Foreign producers not listed in a petition continue to pay their

47. *See* 19 C.F.R. § 351.213 (2011) (describing the administrative review procedure as the most frequently used method of retrospectively calculating final duty liability after goods are imported); *see also* Daniel Ikenson, *Tony Soprano Meets the Antidumping Law*, CATO INST. (Feb. 18, 2011, 12:18 PM), http://www.cato-at-liberty.org/tony-soprano-meets-the-antidumping-law/ (distinguishing the United States as the only major economy to determine 'retrospectively' final AD liability).

48. 19 C.F.R. § 351.213.

49. *See* Pierce & DeFrancesco, *supra* note 1 (describing Commerce's sampling of certain "mandatory" respondents to determine actual import practice).

50. JACKSON, DAVEY & SYKES, *supra* note 15, at 767; *see* Macrory, *supra* note 8, at 28–29 (indicating that Customs refunds or collects the difference between the cash deposits paid by foreign producers and the liquidated amount, plus interest).

51. JACKSON, DAVEY & SYKES, *supra* note 15, at 767.

52. Macrory, *supra* note 8, at 28–29.

53. JACKSON, DAVEY & SYKES, *supra* note 15, at 767.

54. *See* Ikenson, *supra* note 47 (clarifying that neither domestic nor foreign companies are required to request reviews).

55. *See* 19 C.F.R. § 351.213(d)(1) (explaining that petitions for review may be lawfully withdrawn within ninety days and that the administrative review ceases upon a timely withdraw of the petition, with no changes in the duty rates).

56. *See* Macrory, *supra* note 8, at 27–29 (noting that a petition for review must specify which foreign producers to review).

original rates, but those chosen for review face greater uncertainty about their future liability.[57] Also, domestic interested parties may choose to withdraw only a petition for specific foreign producers while continuing the review process against others.[58]

U.S. AD law does not contemplate private-to-private post-order settlements for administrative reviews.[59] Nonetheless, these settlements are increasingly common, and neither Commerce nor the ITC have taken a stance on their permissibility despite, or perhaps because of, their antitrust implications.[60]

D. Like AD Laws, Antitrust Laws Promote Fair Competition

That the ITC and Commerce avoid addressing the antitrust concerns related to private post-order AD settlements does not imply that antitrust concerns do not exist or are not worth investigating.[61] Decades of court decisions recognize that America's national economic policy centers on faith in the value of fair competition.[62] Consequently, U.S. antitrust laws support a general policy that fair trade is desirable.[63] Alongside this broad public interest in maintaining fair competition, courts established that there is a legitimate state interest in identifying and regulating injurious practices in commercial affairs.[64] Therefore, to protect competition and promote

57. *See* JACKSON, DAVEY & SYKES, *supra* note 15, at 767 (noting that requests for review occur in fifty to sixty percent of AD cases).

58. *See* KAYE & DUNN, *supra* note 9 (providing examples of where administrative review petitions were withdrawn for some, but not all, foreign producers).

59. *See* 19 U.S.C. § 1673; *see also* Macrory, *supra* note 8, at 24–46 (outlining the statutorily provided-for settlement methods).

60. *See* Lester, *supra* note 4 (noting that the ITC and Commerce did not rule on these settlements because they lacked proper jurisdiction); Pierce & DeFrancesco, *supra* note 1 (observing the increasing prevalence of these settlements).

61. *See* Heath E. Combs, *ITC Member Scrutinizes Settlement Agreements*, FURNITURE TODAY (Jan. 18, 2011), http://www.furnituretoday.com/article/534949-ITC_member_scrutinizes_settlement_agreements.php (explaining that the ITC only "sidestepped" addressing the legality of these settlements because of their antitrust nature).

62. *See, e.g.*, Standard Oil Co. v. FTC, 340 U.S. 231, 248 (1951) (establishing, in the immediate wake of the Sherman Act, that American economic policies rely on principles of fair competition); *see also* FTC v. Ticor Title Ins. Co., 504 U.S. 621, 632 (1992) (maintaining that the preservation of a fair market free of price fixing or cartels is essential to American principles of economic freedom).

63. *See* Timken Roller Bearing Co. v. United States, 341 U.S. 593, 599 (1951) (reiterating that antitrust legislation reflects the policy that international trade is both possible and necessary).

64. *See* Alt. Pioneering Sys., Inc. v. Direct Innovative Prods., Inc., 822 F. Supp. 1437, 1445 (D. Minn. 1993) (finding a public interest in fostering open and fair competition); Allied Artists Pictures Corp. v. Rhodes, 496 F. Supp. 408, 431 (S.D.

public and state interests, U.S. antitrust laws promote trade by suppressing unfair attempts to hinder competition.[65]

1. *The Sherman Act Is the Primary Piece of U.S. Antitrust Legislation at Issue in AD Cases*

Generally, the Sherman Act prohibits "[e]very contract, combination . . . or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations."[66] For a court to find antitrust liability under the Sherman Act, three elements must be satisfied: (1) at least two parties must have been acting together as a conspiracy; (2) the co-conspirators must have intended to unreasonably restrain trade; and (3) a party must have suffered actual injuries resulting from the restraint in trade.[67]

2. *The Federal Trade Commission Act Expands upon the Sherman Act*

The Federal Trade Commission Act ("FTC Act") prohibits unfair or deceptive practices affecting commerce and is used to prosecute conduct that directly violates the Sherman Act or otherwise violates the "spirit" of U.S. antitrust laws.[68] The Sherman Act and the FTC Act apply to both domestic and foreign firms that restrain either domestic or foreign commerce.[69]

E. Private Settlements Can Violate Antitrust Laws

Generally, private settlement agreements raise antitrust concerns when the agreements involve implications for pricing standards or market

---

Ohio 1980) (holding that states have a legitimate interest in regulating commercial affairs that restrain competition).

65. *See, e.g.*, Balian Ice Cream Co. v. Arden Farms Co., 104 F. Supp. 796, 801 (S.D. Cal. 1952) (accentuating the relationship between antitrust concerns, competition, and trade).

66. Sherman Antitrust Act, 15 U.S.C. § 1 (2006).

67. *See, e.g.*, Coalition for ICANN Transparency, Inc. v. VeriSign, Inc., 611 F.3d 495, 501–02 (9th Cir. 2009) (amend. July 9, 2012) (describing the three elements necessary to state a claim under Section 1 of the Sherman Act); *accord* A Fisherman's Best, Inc. v. Rec. Fishing Alliance, 310 F.3d 183, 189 (4th Cir. 2002) (using similar elements to establish Sherman Act liability).

68. *See* 15 U.S.C. §§ 41–45; Calvani & Tritell, *supra* note 11 (viewing the FTC Act as an extension of the Sherman Act).

69. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST ENFORCEMENT GUIDELINES FOR INTERNATIONAL OPERATIONS 2–4 (Apr. 1995), *available at* 1995 WL 1146233. *See* Empagran S.A. v. F. Hoffmann-LaRoche, Ltd., 417 F.3d 1267, 1269 (D.C. Cir. 2005) (explaining that the Foreign Trade Antitrust Improvements Act creates limited Sherman Act liability for foreign conduct that harms domestic commerce).

allocation.[70] In such cases, the settlement itself may be considered a conspiracy in restraint of trade that violates antitrust law.[71] For example, in *Music Center v. Prestini Musical Instrument Company*, a foreign firm claimed that a U.S. competitor threatened to request an AD investigation if the foreign firm did not accept specific terms.[72] Though the court did not rule on the merits of the collusion via threat of an AD petition, it noted that an AD settlement affecting either the price or quantity of subject imports would violate U.S. antitrust laws.[73]

F. Abuse of Process Implications Can Heighten Antitrust Concerns

Abuse of process concerns arise when a private party uses a legal process against another party to serve a purpose for which that process was not designed.[74] The common law tort of abuse of process is closely related to antitrust concerns because courts can impose antitrust liability upon a party initiating a legal process to hurt its competition instead of using that process for its legitimate and intended purposes.[75] The most common method of abuse of process in antitrust cases is some form of extortion, in which one party uses a legal or administrative process to compel another party to make some sort of payment or to take some specific action that it would not have otherwise.[76] Under an abuse of process standard, the unlawful use of legal action to restrain trade can constitute anticompetitive

---

70. *See* United States v. Singer Mfg. Co., 374 U.S. 173, 175 (1963) (finding Sherman Act antitrust liability for firms using collusive license agreements to disrupt a competitive market); *see also* Andrx Pharm., Inc. v. Biovail Corp. Int'l, 256 F.3d 799, 816 (D.C. Cir. 2001) (indicating that efforts to keep competitors out of a market violate antitrust laws).

71. *See* KAYE & DUNN, *supra* note 9, § 31:1 n.2 (observing that AD settlements necessarily involve relative pricing schemes amongst competitors and pointing to similar private settlement circumstances where such schemes were themselves found to violate antitrust laws).

72. *See* 874 F. Supp. 543, 543, 547 (E.D.N.Y. 1995) (addressing issues of unfair trading, trade secrets, abuses of process, wrongful proceedings, and prima facie torts).

73. *See* Christopher T. Taylor, *The Economic Effects of Withdrawn Antidumping Investigations*, FED. TRADE COMM'N 1, 2 (2001), http://www.ftc.gov/be/workpapers/wp240.pdf (explaining the decision in *Music Center*). *See generally Music Center*, 874 F. Supp. 543 (noting that private agreements involving price fixing, price lists, and quantity allotments can create antitrust liability).

74. *See* RESTATEMENT (SECOND) OF TORTS § 682 (1977).

75. *See id.* § 682 cmt. b; Calvani & Tritell, *supra* note 11, at 532–33 (quoting James D. Hurwitz, *Abuse of Government Processes, the First Amendment, and the Boundaries of* Noerr, 74 GEORGETOWN L.J. 601 (1985)); *see also* Grip-Pak, Inc. v. Illinois Tool Works, Inc., 694 F.2d 466, 471–73 (7th Cir. 1982) (using an abuse of process analysis to propose that courts should focus more on the petitioning parties' subjective intent to harm competition).

76. RESTATEMENT (SECOND) OF TORTS § 682 cmt. b.

conduct subject to antitrust liability.[77]

In *Grip-Pak, Inc. v. Illinois Tool Works, Inc.*, the Seventh Circuit found that even if legal procedures have a legitimate basis in the law, such procedures can still amount to an actionable restraint of trade because an overt harassment of competitors via legal procedures qualifies as an abuse of process that could violate antitrust laws.[78] As Judge Posner explained, for an abuse of process to be actionable under antitrust laws, it does not have to be "malicious" in the tort sense, nor must there be a lack of probable cause for the legal action.[79] The court found, instead, that antitrust concerns arise when a plaintiff does not care about the outcome of the suit itself and is instead concerned with maintaining the suit to force a competitor to perform some act it would not otherwise perform.[80] Though the Supreme Court effectively overruled *Grip-Pak* in *Professional Real Estate Investors, Inc. v. Columbia Pictures Industries, Inc.*,[81] Judge Posner's analysis established the idea that litigation supported by improper anticompetitive purposes should not necessarily be immunized from antitrust liability just because the claim is not entirely baseless.[82]

G. The Noerr-Pennington Doctrine Provides an Important Immunity from Antitrust Liability

The Noerr-Pennington doctrine arose out of two Supreme Court decisions as a judicially created means of exemption from antitrust liability for most lawful attempts to obtain government action.[83] The First

77. *See* Scooter Store, Inc. v. SpinLife.com, LLC, 777 F. Supp. 2d 1102, 1116 (S.D. Ohio 2011) (holding that a firm using trademark litigation to destroy competition was engaged in anticompetitive conduct); *see also* Clipper Exxpress v. Rocky Mountain Tariff Bureau, Inc., 690 F.2d 1240, 1251 (9th Cir. 1982) (explaining that the intentional harassment of competitors through administrative processes creates the same antitrust liabilities as harassing competitors through the judicial system).

78. *See Grip-Pak, Inc.*, 694 F.2d at 471–72 (insisting that the defendant's suit was not necessarily barred by the Noerr-Pennington doctrine simply because the suit was non-malicious).

79. *Id.*

80. *See id.* at 472 (noting the difficulty of drawing lines between lawful and unlawful competitive purposes in filing a suit).

81. *See generally* Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc., 508 U.S. 49 (1993) (discussing that a plaintiff's subjective intent was not relevant in an antitrust case involving otherwise lawful litigation unless the plaintiff's suit was first found to be objectively unreasonable).

82. *See Grip-Pak, Inc.*, 694 F.2d at 471 ("If abuse of process is not constitutionally protected, no more should litigation that has an improper anticompetitive purpose be protected, even though the plaintiff has a colorable claim.").

83. *See* United Mine Workers v. Pennington, 381 U.S. 657 (1965); E. R.R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127 (1961); *see also* Thomas J. Prusa, *Why Are So Many Antidumping Petitions Withdrawn?*, 33 J. INT'L

Amendment strongly influenced the doctrine's limitations on antitrust liability.[84] Under this doctrine, as long as a private party petitions the government for a lawful form of redress, that party is exempted from antitrust scrutiny, even if the petitioned-for government action might harm competition.[85] Noerr-Pennington protection extends to cover private parties' petitions that result in settlement agreements between the petitioning parties and the government.[86]

When assessing the scope of Noerr-Pennington's antitrust liability protection, courts look at the impact, source, context, and nature of the anticompetitive activity at issue.[87] However, even if the underlying purpose of the activity is to achieve an anticompetitive restraint of trade, the Noerr-Pennington doctrine immunizes that activity from antitrust liability so long as it is a lawful solicitation of government action.[88] Though many courts hold that a petitioner's "bad intent or anticompetitive motivation" in seeking government action is "irrelevant" for purposes of Noerr-Pennington protection, others question this reasoning.[89]

ECON. 1, 6–7 (1992) (describing the Noerr-Pennington doctrine's origins).

84. *E.g.*, *Grip-Pak, Inc.*, 694 F.2d at 471; *see* Prusa, *supra* note 83, at 6–7 (clarifying that under the Noerr-Pennington doctrine, antitrust liability is subordinate to the constitutionally protected right to petition any branch or department of government, or otherwise participate in the legislative process).

85. *See* Cho, *supra* note 5, at 361 (explaining that any anticompetitive effects of a lawful petition are irrelevant for Noerr-Pennington purposes).

86. *See* VIBO Corp., v. Conway, 669 F.3d 675, 683–84 (6th Cir. 2012) (explaining that the actions protected by the Noerr-Pennington doctrine include settling with the government, but making no mention of private-to-private settlement agreements). *But cf.* Cho, *supra* note 5, at 361 (arguing that courts interpret the Noerr-Pennington doctrine so narrowly that its protections would probably extend to cover private AD settlements).

87. *See* Allied Tube & Conduit Corp. v. Indian Head, Inc., 486 U.S. 492, 504 (1988).

88. *See* Freeman v. Lasky, 410 F.3d 1180, 1184 (9th Cir. 2005) (stating that "conduct incidental to" a petition is still protected by the Noerr-Pennington doctrine so long as the petition itself would be protected); Marina v. Fisher, 338 F.3d 189, 197 (3rd Cir. 2003) (emphasizing that Noerr-Pennington immunity protects lawful petitioning of government regardless of improper motives); *Grip-Pak, Inc.*, 694 F.2d at 471 (asserting that the *Noerr* Court viewed collective efforts to influence legislation as a form of petitioning, regardless of their purpose).

89. *Compare* Assoc. Container Transp. Ltd. v. United States, 705 F.2d 53, 58–59 (2d Cir. 1983) (stating that lawful efforts to influence government are immune from Sherman Act liability regardless of anticompetitive purposes), *and VIBO Corp.*, 669 F.3d at 684 (holding that subjective anticompetitive intent is irrelevant in Noerr-Pennington determinations), *with Grip-Pak, Inc.*, 694 F.2d at 471–72 (proposing that subjective intent should be given more consideration in Noerr-Pennington decisions).

H. Shams: An Exception to the Noerr-Pennington Rule

Noerr-Pennington immunity is not absolute because courts created a 'sham' exception, which removes the doctrine's protection for 'sham' petitions that are solely intended to hurt competition.[90] Specifically, the sham exception applies when parties use a governmental process itself, instead of the outcome of that process, as an anticompetitive weapon.[91]

Traditionally, courts use a two-prong test to determine whether a petition for lawful governmental action qualifies as a sham: (1) the petition must be objectively baseless; and (2) the petitioner's subjective motivation must be to conceal its intent to use the governmental process for anticompetitive purposes.[92] If both prongs are satisfied, courts will not afford petitioners the Noerr-Pennington doctrine's antitrust immunity.[93]

Some courts characterize the use of sham actions as a form of "abuse of process."[94] For instance, Justice Stevens, in his *Professional Real Estate Investors* concurrence, recognized that many sham cases involve an abuse of process, and he argued that the distinction between sham and genuine litigation should not be the only difference between lawful and unlawful conduct.[95] As Justice Stevens explained, the sham exception's objective

---

90. Cho, *supra* note 5, at 361. *See generally* Prof'l Real Estate Investors, Inc., v. Columbia Pictures Indus., Inc., 508 U.S. 49 (1993) (applying the sham exception).

91. *See VIBO Corp.*, 669 F.3d at 685–86 (differentiating between using a lawful process itself and the outcome of a process to harm competitors); *In re* Tamoxifen Citrate Antitrust Litig., 429 F.3d 370, 401 (2nd Cir. 2005) (insisting that Noerr-Pennington immunity applies when an anticompetitive effect is a consequence of some governmental action, but not the means for obtaining such action); Winterland Concessions Co. v. Trela, 735 F.2d 257, 263–64 (7th Cir. 1984) (quoting Gainsville v. Florida Power & Light Co., 488 F. Supp. 1258, 1265–66 (S.D. Fla. 1980)) ("[T]he prerequisite motive for the sham exception is the intent to harm one's competitors not by the *result* of the litigation but by the simple fact of the *institution* of the litigation." (emphasis maintained)).

92. *See Prof'l Real Estate Investors, Inc.*, 508 U.S. at 60–61 (1993) (establishing the two-prong test for defining sham litigation under Noerr-Pennington, holding that courts must satisfy the first prong—that the petition was objectively baseless—before examining a petitioner's subjective intent, and explaining that objectively baseless petitions occur if a petition has no reasonable expectation of success on its merits).

93. *See* Calvani & Tritell, *supra* note 11, at 536–37 (using a hypothetical situation to explain how courts conduct Noerr-Penning sham analyses).

94. *See* Clipper Exxpress v. Rocky Mountain Motor Tariff Bureau, Inc., 690 F.2d 1240, 1259 (9th Cir. 1982) (holding that some form of abuse of process must be found in order to invoke the sham exception); *Grip-Pak, Inc.*, 694 F.2d at 471–72 (comparing the Noerr-Pennington doctrine to the tort of abuse of process and applying abuse of process standards to show that litigation can be improper even if it is supported by probable cause); Ad Visor, Inc. v. Pac. Tel. & Tel. Co., 640 F.2d 1107, 1109 (9th Cir. 1981) (examining Noerr-Pennington case law and characterizing courts' sham exception analyses as tests for an abuse of process).

95. *See Prof'l Real Estate Investors, Inc.*, 508 U.S. at 75–76 (1993) (Stevens, J.,

reasonableness test may not be appropriate for determining the lawfulness of a petition in complicated antitrust cases involving an abuse of process.[96]

Judge Posner, in *Grip-Pak*, partially inspired Justice Stevens's reasoning by questioning other courts' use of the Noerr-Pennington doctrine to grant antitrust immunity to parties petitioning the government for purely anticompetitive purposes.[97] Employing an abuse of process analysis, Judge Posner reasoned that if Noerr-Pennington immunity is applied too broadly—to the point that all non-malicious litigation is immunized from government regulation—the tort of abuse of process will itself become unconstitutional.[98] Judge Posner further noted that the language surrounding abuse of process laws precisely embodies the types of legal activity that courts usually do not protect under the First Amendment.[99]

Other courts offer varying interpretations on the scope of the Noerr-Pennington sham exception.[100] For instance, the court in *Music Center* held that a domestic firm's filing of multiple AD and administrative review petitions against its foreign competitors did not qualify as a sham activity because there was no evidence that the domestic firm lacked a reasonable expectation of success on the merits of its petition.[101] Additionally, three U.S. courts of appeals require that shams be legally unreasonable, others hold that no successful litigation can be a sham, and still other courts of appeals consider some meritorious litigation to be a sham.[102]

---

concurring) (providing examples of how objectively reasonable lawsuits can still violate antitrust laws).

96. *See id.* at 74–76 (building upon the abuse of process analysis in *Grip-Pak*, disagreeing with the majority's equation of objective baselessness, and encouraging the Court to avoid making unnecessarily broad holdings in complicated sham exception cases).

97. *See Grip-Pak, Inc.*, 694 F.2d at 470–71 (evaluating whether a lack of probable cause is necessary to create actionable antitrust liability).

98. *See id.* at 471 (examining the Supreme Court's analysis in California Motor Transp. Co. v. Trucking Unlimited, 404 U.S. 508, 510 (1972)).

99. *Id.*

100. *Prof'l Real Estate Investors, Inc.*, 508 U.S. at 55 n.3 (1993) (explaining how the various courts of appeals apply different standards in their Noerr-Pennington sham analyses).

101. *See* Music Center S.N.C. Di Luciano Pisoni & Co. v. Prestini Musical Instruments Corp., 874 F. Supp. 543, 549–50, 554–55 (E.D.N.Y. 1995) (holding that the domestic firm would be immune from liability, even if the sole purpose of its petition was to injure a foreign competitor).

102. *Prof'l Real Estate Investors, Inc.*, 508 U.S. at 55 n.3 (1993) (acknowledging various courts of appeals' inconsistent and often contradictory definitions of "sham" litigation).

I. The Chinese Furniture Case Reveals How AD Investigations Actually Operate

In October 2003, an ad hoc association of twenty-seven U.S. furniture producers filed AD petitions with Commerce and the ITC concerning imports of certain wooden bedroom furniture from China.[103] After a full investigation, Commerce made an affirmative determination, finding that wooden bedroom furniture imports from China were being dumped in the U.S. market at LTFV.[104] The ITC found that the LTFV imports of Chinese furniture materially injured the domestic wooden furniture industry.[105] Commerce issued an AD order with respect to imports of certain wooden bedroom furniture from China on January 4, 2005.[106] From then on, cash deposits accompanied all imports of wooden bedroom furniture from China.[107] Commerce assigned different cash deposit rates to Chinese furniture producers depending on their estimated dumping margins, but because so many Chinese producers were included in the investigation, Commerce applied its sampling procedure; thus, some producers received lower individualized rates, but most Chinese producers received the much higher "China-wide" duty rate.[108]

By the ITC's first sunset review of the orders in December 2009, Commerce had already completed four administrative reviews, with a fifth review pending.[109] When choosing which Chinese producers to review, the domestic interested parties petitioned for reviews of nearly every Chinese producer with relatively low deposit rates.[110] For the firms not listed in the

---

103. *See* Chinese Furniture, *supra* note 2, at I-2 & n.6.

104. Final Determination of Sales at Less Than Fair Value: Wooden Bedroom Furniture From the People's Republic of China, 69 Fed. Reg. 67, 313 (Dep't of Commerce Nov. 17, 2004); Chinese Furniture, *supra* note 2, at I-2.

105. Wooden Bedroom Furniture from China, 69 Fed. Reg. 77, 779 (Int'l Trade Comm'n Dec. 28, 2004); Chinese Furniture, *supra* note 2, at I-2.

106. Notice of Amended Final Determination of Sales at Less Than Fair Value and Antidumping Duty Order: Wooden Bedroom Furniture From the People's Republic of China, 70 Fed. Reg. 329 (Int'l Trade Admin. Jan. 4, 2005).

107. *See generally* Chinese Furniture, *supra* note 2 (describing the history of the AD orders on certain wooden bedroom furniture from China and the associated duty payments).

108. *See* Chinese Furniture, *supra* note 2, at tbl. I-2 (displaying the various margins assigned to specific Chinese furniture producers, ranging between 0.4% and 39.46% as well as the "PRC-Wide Rate" of 216.01% that was assigned to the majority of Chinese producers under Commerce's sampling procedures).

109. Chinese Furniture, *supra* note 2, at I-8 to I-10, app. E.

110. *See* Posthearing Brief of Guandong Furniture Ass'n at 10, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Dec. 2010) (Review) (revealing that, on average, domestic interested parties requested reviews of 158 Chinese producers in each administrative review petition).

petitions for review, Commerce automatically applied the duty rates assessed from the original investigation or the previous administrative reviews.[111] For firms listed in the petitions, Commerce investigated the past years' import data and calculated new dumping margins.[112] Every year, however, most Chinese producers reached settlement agreements with the domestic interested parties, and the domestic parties removed every Chinese producer that settled from the petition for review.[113]

II. THE ADMINISTRATIVE REVIEW PROCESS INCENTIVIZES QUESTIONABLY LEGAL SETTLEMENT AGREEMENTS THAT FRUSTRATE THE OBJECT AND PURPOSE OF EXISTING AD LAWS

This Section explores how the inherent uncertainty of AD administrative reviews creates a system in which domestic firms can pressure their foreign competitors into post-order settlement agreements that put cash in the pockets of domestic producers. This Section then analyzes how these collusive settlements generate important antitrust concerns that are, however, likely mitigated by insufficiently particular AD laws and courts' narrow application of the Noerr-Pennington doctrine. This Section also describes how, antitrust legality notwithstanding, these settlements run afoul of the intended goals of AD orders and frustrate the object and purpose of existing AD legislation.

A. Through Uncertainty, the Administrative Review Process Opens the Door to Cash Settlement Payments

Under the United States' unique retrospective AD duty assessment system, subject foreign producers begin paying AD duties immediately after affirmative final determinations by Commerce and the ITC, but their final liability is often unknown for more than another year.[114] Thus, the real sting of an AD order is in the inherent uncertainty of the hard-to-predict final duty liability because the opaque administrative review process may ultimately require foreign producers to retroactively pay much higher duty rates.[115]

Commerce's AD investigations and administrative reviews are,

111. *See* Chinese Furniture, *supra* note 2, at I-8 n.14.

112. *Id.* at I-8 n.14, I-9.

113. *Id.* at 16, III-2, III-3.

114. *See* Ikenson, *supra* note 47 (noting that final liability determinations may be delayed for as long as eighteen months, or even, sometimes, for several years).

115. *See* AFMC's Answers to Commissioners' Questions at 41, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058 (Dec. 2010) (Review) (arguing that final liability uncertainty harms foreign producers by raising their transaction costs).

therefore, extremely costly for foreign producers—often generating millions of dollars in legal fees—and their outcomes are difficult to predict.[116] This is especially true when domestic parties petition for reviews of many foreign firms, causing Commerce to employ its sampling techniques to determine dumping margins.[117] In addition to the upfront legal fees and costs of satisfying the administrative review requirements, subject foreign producers face costly uncertainty over their ultimate AD duty liabilities.[118] Domestic interested parties use this heightened uncertainty to pressure foreign producers into accepting collusive settlement agreements.[119] The burden of administrative reviews' unpredictable costs is so large that the mere threat of a review petition often causes subject foreign producers to settle.[120]

When settling, domestic interested parties and subject foreign producers work out a system in which the foreign producers that agree to make cash payments to domestic producers are removed from the administrative review petition; thus, those foreign producers retain their prior, and thus predictable, duty rates.[121] These agreements are especially effective because domestic interested parties target foreign producers paying relatively low duty rates and who thus are especially fearful of the much higher country-wide duty rates.[122]

At first, it may seem that domestic interested parties would not pursue such agreements because they do nothing to curtail the harmful effects of dumped subject foreign imports; however, these agreements do provide domestic interested parties with something that past trade laws conditioned them to associate with AD orders—cash.[123] Congress's repeal of the Byrd

116. KAYE & DUNN, *supra* note 9; Cho, *supra* note 5, at 388.

117. *See* Pierce & DeFrancesco, *supra* note 1 (detailing how the broad spectrum of firms included in the sampling process makes it more difficult to predict what new duty rates might be).

118. KAYE & DUNN, *supra* note 9.

119. *See id.*, *supra* note 9 (describing how domestic producers consciously leverage the heightened uncertainty of administrative reviews to encourage settlements and how foreign producers view their original deposits as 'sunk costs' that they weigh against the uncertainty of administrative reviews).

120. *See* B. Peter Rosendorff, *Voluntary Export Restraints, Antidumping Procedures, and Domestic Politics*, 86 AM. ECON. REV. 544, 544–45 (1996) (observing that petitions for review are withdrawn for nearly one-third of all subject foreign producers in AD cases, and nearly every withdrawal is associated with a private settlement agreement). *Cf.* Cho, *supra* note 5, at 396 (describing the uncertainty costs of non-price predation).

121. Ikenson, *supra* note 47; Pierce & DeFrancesco, *supra* note 1.

122. *See* INT'L TRADE ADMIN., *supra* note 36, at 4; Hagerty, *supra* note 2.

123. *See* Pierce & DeFrancesco, *supra* note 1 (noting that, because of the Byrd Amendment, domestic producers grew accustomed to receiving cash from AD orders).

Amendment forced domestic industries to look elsewhere for easy cash. Their solution? Private settlement agreements.[124]

Overall, four key factors enable these private post-order settlement agreements: (1) relatively low AD rates that exporters do not want to see increase; (2) annual petitions for review of nearly every subject foreign producer; (3) Commerce's use of sampling to assign duty rates; and (4) the absence of Byrd Amendment payouts.[125]

1. *The Chinese Furniture Case Reveals the Full Extent and Effects of These Settlements*

The Chinese furniture case demonstrates how AD rules and procedures enable private post-order settlement agreements and reveals the full extent and effects of these settlements. Every year after Commerce issued the original AD duty order, the domestic furniture industry took advantage of Commerce's administrative review system and submitted petitions for the review of hundreds of Chinese furniture producers.[126] The domestic industry used those petitions to induce Chinese producers to enter into lucrative settlement agreements in which the domestic industry removed Chinese producers from the petition if they agreed to pay cash to the domestic producers.[127] Knowing that many Chinese producers could tolerate their current rates and would like to avoid paying the much higher China-wide duty rate, the domestic producers conveyed to the Chinese producers that the petitions would be withdrawn if they agreed to pay off the domestic producers.[128] This extortive process was so effective that

124. *See id.* (pointing to the repeal of the Byrd Amendment as an incentive for AD settlement agreements).

125. *Id.*

126. *See* Prehearing Brief of Dalian Haufeng Furniture Group at 9, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Dec. 2010) (Review) (describing the domestic furniture industry as "strategic" and "coordinated" in their efforts to compel settlements with Chinese competitors).

127. *See id.* (describing these settlements as a "reward" for the Chinese producers willing to either enter into exclusive trading arrangements with domestic producers or make settlement payments, and, in contrast, describing the review process as a punishment for those Chinese producers refusing to settle); *see also* Posthearing Brief of Guandong Yihua Timber Industry Co., Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203, at 10–11 (Dec. 2010) (Review) (providing a first hand account of how domestic furniture producers refused to remove one company from an administrative review petition because it would not settle; thus, that company was selected as a mandatory respondent and subjected to higher rates).

128. *See* Posthearing Brief of Furniture Retailers of America at 3–4, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Dec. 2010) (Review) (explaining that domestic furniture producers "let it be known" that they would withdraw administrative review petitions, effectively preserving original duty rates of 7.24% or less, for Chinese producers willing to meet the domestic petitioners

within five years of the original order, a majority of Chinese furniture producers chose to settle with domestic producers.[129] Over that time, Chinese furniture producers paid tens of millions of dollars to twenty domestic furniture producers in exchange for removing their names from the petitions for review.[130]

Domestic producers carefully calculated the size of each Chinese producers' settlement payments as a percentage of the value of each producers' imports.[131] This incentivized domestic interested parties to encourage more subject imports because higher import volumes meant even larger settlement payments.[132] This calculation method, however, was not strictly standardized, and some Chinese furniture producers received discounted settlements because of their special commercial relationships with domestic producers.[133]

B. These Increasingly Common Private Post-Order Settlements Raise Far-Reaching Legal Concerns

Though the ITC only recently recognized the existence of these settlements, economists long suspected that withdrawals of AD petitions

---

settlement terms); Ikenson, *supra* note 47 (describing the domestic industry's exploitation of those Chinese producers that could tolerate the duties they were already paying as "clever shakedowns"); *see also* Transcript, *supra* note 3, at 196 (Leslie Thompson, owner of an American furniture firm with production facilities in China, recounting a conversation with an attorney for the domestic interested parties where he "asked [her] what [she] could give him that would entice his client, the Petitioners, to drop [her firm] from the review"); Ellen Croibier, *From China, an end run around U.S. tariffs*, TRADEREFORM.ORG (May 23, 2011), http://www.tradereform.org/2011/05/6233/ (noting that once Chinese producers paid the domestic firms, they were dropped from the review petitions).

129. *See* Chinese Furniture, *supra* note 2, at III-2, III-3; Posthearing Brief of Guandong Furniture Ass'n, *supra* note 110, at 10 (revealing that domestic interested parties withdrew fifty-one percent of subject Chinese producers from the first review petitions, seventy-nine percent from the second review, ninety-one percent from the third review, and eighty-nine percent from the fourth review, and all withdrawals were made in exchange for making cash payments to the domestic producers).

130. Posthearing Public Report to Commission at III-10, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Dec. 2010) (Review). *Cf.* Ikenson, *supra* note 47 (noting that an even larger, unspecified amount of money was paid directly to the domestic interested parties' attorneys).

131. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 4, 7 (reflecting the understanding of the Furniture Retailers of America after their investigation of Commerce's import data and specific annual settlement amounts).

132. *See id.* at 7 (describing the "perverse incentives" produced by the order and how these settlements allowed domestic producers to increase their profit without re-employing any workers to curtail the harmful effects of subject imports).

133. *See id.* at 63 (claiming domestic firms use special commercial relationships to effectively regulate import volumes).

signaled some type of collusive agreement between domestic and foreign producers.[134] Those economists were largely correct because the settling of administrative reviews is not new, and the prevalence of private post-order settlement agreements is growing rapidly.[135] Notably, in every recent AD case involving post-order settlement agreements, the domestic interested parties represented such sufficiently aligned interests that the domestic industry could speak with one voice and control the process of submitting and withdrawing the petitions for review; it is not clear whether this settlement scheme will work if domestic interested parties are unorganized or divided in their goals or motives.[136]

1. The Collusive Nature of These Settlements Raises Many Antitrust Concerns

Fair competition is a central tenant of U.S. economic policy, and U.S. antitrust laws support this policy by protecting both domestic and foreign competition.[137] Therefore, actions that encourage unfair trade or disrupt market competition raise serious antitrust concerns.[138] U.S. trade law accounts for two primary methods of settling AD cases, and Commerce must oversee both methods.[139] In contrast, private post-order settlements are conducted without any agency oversight.[140] Without agency oversight, any discussion of price or quantity restraints runs significant risks of

134. Cho, *supra* note 5, at 394; *see* Combs, *supra* note 61 (noting that although the ITC formally recognized the settlement process in the furniture case, Commerce continues to deny knowledge of their existence).

135. *See* Ikenson, *supra* note 47 (explaining that these agreements operated "in the shadows" for years). *Cf.* Pierce & DeFrancesco, *supra* note 1 (tracing the rise of these settlements back to the Byrd Amendment and its repeal).

136. *See* Pierce & DeFrancesco, *supra* note 1 (questioning whether these settlement schemes will be as effective if domestic industries are less organized); *see also* KAYE & DUNN, *supra* note 9 (noting that no public or private party has yet challenged these post-order AD settlement agreements in court).

137. *See* Standard Oil Co. v. FTC, 340 U.S. 231, 248 (1951) (establishing that American economic policy relies on principles of fair competition); Balian Ice Cream Co. v. Arden Farms Co., 104 F. Supp. 796, 801 (S.D. Cal. 1952) (connecting antitrust concerns with fair trading practices).

138. *See* Calvani & Tritell, *supra* note 11, at 530–31 (illustrating how the most pressing issues arise when private AD settlement agreements bring about collusive outcomes because antitrust violations are "unavoidable" when domestic and foreign firms act together to restrain trade).

139. *See* 19 U.S.C. § 1673c(d)(1) (establishing a public interest requirement for suspending an AD investigation); Macrory, *supra* note 8, at 24–25 (explaining that suspension agreements and AD petition withdrawals both require Commerce's approval before AD cases can be 'settled').

140. KAYE & DUNN, *supra* note 9.

violating antitrust laws.[141]

The most prominent piece of antitrust legislation at issue is the Sherman Act, which explicitly prohibits collusive acts that restrain trade or harm competition.[142] Post-order AD settlement agreements run afoul of the three central elements of the Sherman Act.[143] First, the Sherman Act's contract, combination, or conspiracy element is easily satisfied: because these settlements involve direct agreement and cooperation amongst foreign and domestic industries, and each of those industries is comprised of multiple firms, there are almost always multiple parties acting together to restrain trade.[144] Second, the restraint of trade or commerce element is satisfied because these private settlement agreements usually involve some type of relative pricing or quantity agreement amongst market participants.[145]

Finally, the restraints on trade caused by the post-order settlements inflict actual injuries on certain foreign and domestic competitors, satisfying the final element for antitrust liability under the Sherman Act.[146] Domestic producers not participating in the AD case suffer because they do

141. *Cf.* KAYE & DUNN, *supra* note 9 (recounting how, in an AD case involving a private settlement agreement, there were no antitrust concerns because neither the negotiations nor the agreement involved any market price or quantity restrictions).

142. 15 U.S.C. § 1.

143. *See* Coalition for ICANN Transparency, Inc. v. VeriSign, Inc., 611 F.3d 495, 501–02 (9th Cir. 2009) (describing the three primary requirements for stating a claim under the Sherman Act: the existence of a conspiracy, intent to restrain trade, and actual injury to competition or trade).

144. *See* A Fisherman's Best, Inc. v. Rec. Fishing Alliance, 310 F.3d 183, 189 (4th Cir. 2002) (explaining that for success on a claim alleging violations of the Sherman Act, a plaintiff must show that two persons acted in concert and that their actions constituted an unreasonable restraint on commerce); Calvani & Tritell, *supra* note 11, at 546 (clarifying that, under the Sherman Act, there cannot not be an antitrust violation if a single firm petitions the government in an effort to restrain trade or commerce because there could not possibly be two or more actors joined under a contract, combination, or conspiracy); Cho, *supra* note 5, at 398 (noting that multiple domestic firms discuss prices and costs among themselves when filing AD petitions because the petitions must be filed by a representative number of domestic producers of like products).

145. *See* Music Center v. Prestini Musical Instrument Company, 874 F. Supp. 543, 557 (E.D.N.Y. 1995) (holding that price fixing in order to control market access violates antitrust laws); KAYE & DUNN, *supra* note 9 (noting that AD settlements raise antitrust concerns because they involve relative pricing agreements amongst market participants and explaining that when private settlement agreements involve implications for pricing standards or market allocation, the settlement itself may be considered a conspiracy in restraint of trade); *see also* Taylor, *supra* note 73, at 3 (claiming that, though there is little precedent, a private AD settlement attempting to increase prices or decrease imports, absent some sort of joint venture, is illegal).

146. *See, e.g.*, *Coalition for ICANN Transparency, Inc.*, 611 F.3d at 501–02 (9th Cir. 2009) (holding that, to establish Sherman Act liability, a party must suffer actual injuries resulting from the restraint in trade).

not receive the cash payouts, and the settlement agreements do nothing to limit the flow of unfair subject imports, which continue to injure the sales of their goods in the U.S. market.[147] Moreover, foreign producers with special relationships with the domestic petitioners receive better settlement terms; this effectively raises the relative costs for the foreign producers that receive the relatively less favorable terms by limiting their ability to compete in the U.S. market.[148]

Expanding upon the Sherman Act, the FTC Act raises additional antitrust concerns by imposing antitrust liability on conduct that "violates the spirit" of the Sherman Act.[149] The use of AD settlements to restrain trade violates the "spirit" of the Sherman Act because these settlements represent intentional and collusive efforts to harm competitors and restrain commerce in exchange for economic benefits.[150] This effect epitomizes the exact opposite of the Sherman Act's intended purpose of promoting competition and prohibiting collusive acts that restrain trade.[151]

In addition to straightforward Sherman Act or FTC Act violations, these settlements may create additional liability as an abuse of process.[152] Generally, an abuse of process occurs when a private actor uses a legal process, against another party, primarily to accomplish a purpose for which

147. *See* Chinese Furniture, *supra* note 2, at 29 (Additional Views of Comm'r Daniel R. Pearson) (analyzing the AD order's effects and how the volume of subject Chinese furniture imports remained substantial, in both absolute terms and in terms of relative market share).

148. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 7, 63 (connecting some foreign firms' relatively lower settlement rates with special business relationships); JACKSON, DAVEY & SYKES, *supra* note 15, at 767–68 (affirming that administrative reviews cause foreign producers to face heightened, and costly, uncertainty); *see also* United States v. Singer Mfg. Co., 374 U.S. 174, 193–95 (1963) (finding that collusive efforts to treat specific foreign competitors differently, in order to hurt those competitors' imports to the United States, violated the Sherman Act).

149. *See* Calvani & Tritell, *supra* note 11, at 548–50 (citing Grand Union Co. v. FTC, 300 F.2d 92 (2d Cir. 1962)) (explaining that the FTC Act prohibits unfair or deceptive methods of competition or practices affecting commerce).

150. *Id.* (arguing that the abuse of import relief mechanisms frustrates the intended purpose of the Sherman Act).

151. *See* Standard Oil Co. v. FTC, 340 U.S. 231, 247–50 (1951) (looking to congressional intent surrounding the Sherman Act, and other antitrust laws, to determine that the purpose of antitrust laws is the protection of fair trade and competition).

152. *See* RESTATEMENT (SECOND) OF TORTS § 682 cmt. b (finding that the most common instances of abuse of process, as it relates to antitrust concerns, arise in cases of extortion where one party uses a lawful governmental process to unlawfully pressure its competitors into making some sort of debt payment or partaking in some specific action).

that process was not designed.[153] The intended purpose of the administrative review process is not to transfer wealth from foreign to domestic producers.[154] Rather, the review process is supposed to further the goals of AD laws in general; for example, to protect domestic industries from unfair import competition.[155] The domestic industries' use of administrative reviews to pressure foreign competitors into lucrative settlement agreements is thus not a purpose that the review process was intended to achieve, especially since the repeal of the Byrd Amendment revealed Congress's intent to keep AD duty revenues out of the hands of domestic industries.[156] The review process is supposed to help protect domestic industries, but both domestic production volume and employment decrease after these settlements transpire; thus, the agreements fail to further a primary goal of the administrative review process.[157]

Admittedly, domestic interested parties are well within their rights to file administrative review petitions in most AD cases.[158] However, as Judge Posner proposed in *Grip-Pak*, the use of a legal process does not have to be "malicious" in order to violate antitrust laws, and the use of legal procedures to harass competitors can qualify as an abuse of process that

153. *See id.* § 682.

154. *See* Lester, *supra* note 4 (explaining that the repeal of the Byrd Amendment raises antitrust concerns because domestic producers are not supposed to receive AD duty payments anymore, but through private settlements domestic producers found a way to do what Congress tried to stop).

155. Schnerre, *supra* note 7, at 497–98.

156. *See* Pierce & DeFrancesco, *supra* note 1 (claiming that the Byrd Amendment's repeal incentivized these settlement agreements); Schnerre, *supra* note 7, at 498 (explaining that AD laws only provide administrative remedies and are thus not designed to facilitate direct payments to domestic parties); *see also* Prehearing Brief of Guandong Furniture Ass'n at 5–6, Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203 (Dec. 2010) (Review) (noting that even under the Byrd Amendment, domestic producers were only entitled to AD duty funds through some government action). *But cf.* Tudor N. Rus, Recent Development, *The Short, Unhappy Life of the Byrd Amendment*, 10 N.Y.U. J. LEGIS. & PUB. POL'Y 427, 434–38 (2007) (arguing that international pressure and the WTO played a large part in causing Congress to repeal the Byrd Amendment).

157. *See* Chinese Furniture, *supra* note 2, at 29 (observing the failure of the settlement agreements to improve domestic performance indicators). Moreover, the payments from foreign competitors were only distributed amongst a certain subset of domestic producers, and the domestic industry did not use the funds in an effort to offset the harmful effects of the subject imports. *See id.*; *see also* Croibier, *supra* note 128 (reporting that, in the Chinese Furniture case, the U.S. furniture industry lost jobs at an even faster rate after the settlements began).

158. *See* 19 C.F.R. § 351.213 (showing that domestic parties may have valid interests in petitioning for administrative reviews and explaining the rules for implementing such reviews).

violates antitrust laws.[159] Judge Posner maintained that, even if there is probable cause for pursuing the legal action, petitioning parties could still violate antitrust laws if those parties are not actually concerned with winning a favorable judgment but instead are concerned with harassing competitors.[160] In private administrative review settlements, domestic interested parties are not necessarily concerned about the outcomes of the reviews because, even if the review decisions are not in their favor, they still receive some protection from subject imports because the original AD orders are not removed.[161] Instead, domestic parties are more concerned with using the threat of a costly review process to compel foreign competitors into settling because domestic producers are seeking the cash they grew accustomed to under the Byrd Amendment.[162]

2. *The Noerr-Pennington Doctrine Probably Stands in the Way of Antitrust Liability*

Though post-order settlements of AD cases raise many antitrust concerns,[163] these settlements are likely protected from antitrust liability by the Noerr-Pennington doctrine.[164] Under this doctrine, a private party petitioning the government for some lawful action is generally exempted from antitrust scrutiny, even if the petition acts to restrain commerce.[165] In AD cases, a petition for an administrative review is a lawful action, and domestic interested parties may lawfully pick which foreign firms to include in the review.[166] Moreover, domestic interested parties' withdrawal of a review petition within ninety days is also a lawful action.[167] Thus, petitioning for administrative reviews is lawful under AD law and likely

159. *See* Grip-Pak, Inc. v. Illinois Tool Works, Inc., 694 F.2d 466, 472–73 (7th Cir. 1982) (referring to the "malicious" requirement for the common law tort of abuse of process).

160. *See id.* (claiming that a majority of court decisions on the topic support such an opinion).

161. *See* Macrory, *supra* note 8, at 30–31 (describing the sunset review process, not administrative reviews, as the means by which AD orders can be removed). *Cf.* Prusa, *supra* note 83, at 7 (observing the special role of domestic parties in the administrative review process and proposing that they use their role with the explicit intent to obtain a settlement offer).

162. *See* Pierce & DeFrancesco, *supra* note 1 (tracing the domestic parties' motivations for AD settlements to the Byrd Amendment).

163. *See infra* Section II.B.1.

164. *See, e.g.*, Prusa, *supra* note 83 (proposing that AD settlements are protected by Noerr-Pennington immunity).

165. *See* Cho, *supra* note 5, at 361 (insisting that the Noerr-Pennington doctrine obstructs the Federal Trade Commission's antitrust regulation of trade remedies).

166. *See* Macrory, *supra* note 8, at 27–29.

167. 19 C.F.R. § 351.213(d)(1).

enjoys Noerr-Pennington immunity.

Many courts strictly uphold Noerr-Pennington immunity, even if the petitioning party was motivated by anticompetitive purposes designed to restrain trade.[168] Such a narrow application of the doctrine essentially allows domestic producers to use the administrative review process to extort foreign competitors without any threat of antitrust liability because the doctrine exempts the domestic producers' lawful attempts to obtain government action from any antitrust liability.[169]

However, domestic interested parties do not necessarily enjoy absolute protection from antitrust liability because of the Noerr-Pennington doctrine's "sham" exception.[170] Generally, courts invoke the sham exception in situations where parties use a governmental process itself, and not the outcome of that process, as an anticompetitive weapon.[171] Because courts vary in their application of the Noerr-Pennington sham exception, it is not clear whether AD administrative review petitions filed in an attempt to compel private settlement agreements qualify as a sham for Noerr-Pennington purposes.[172]

Generally, to qualify as a sham, an administrative review petition must fulfill both elements of the two-prong test courts traditionally use to evaluate whether an action falls under the Noerr-Pennington sham exception.[173] First, a court must determine whether the petition was objectively baseless.[174] A petition for administrative review is considered objectively baseless if a court finds that an objective petitioner could not

168. *See* Cho, *supra* note 5, at 361 (reasoning that courts' narrow interpretation of the Noerr-Pennington doctrine's sole exception would make that exception ineffective in AD cases); Associated Container Transp. Ltd. v. United States, 705 F.2d 53, 58–59 (2d Cir. 1983) (considering petitioning parties' subjective motivations to be irrelevant for Noerr-Pennington purposes).

169. *See* Prusa, *supra* note 83 (suggesting that Noerr-Pennington protection effectively provides domestic parties with a "right" to pursue or attain private settlement agreements).

170. *See, e.g.*, Cho, *supra* note 5, at 361 (describing the sham exception as a limitation on the Noerr-Pennington immunity).

171. *See, e.g.*, VIBO Corp., Inc. v. Conway, 669 F.3d 675, 684–85 (6th Cir. 2012); Knology, Inc. v. Insight Commc'n Co., 393 F.3d 656, 658–59 (6th Cir. 2004). *Cf.* California Motor Transp. Co. v. Trucking Unlimited, 404 U.S. 508, 515 (1972) ("If the end result is unlawful, it matters not that the means used in violation may be lawful.").

172. *See* Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc., 508 U.S. 49, 55 n.3 (1993) (observing that several courts of appeals demand that an alleged sham be legally unreasonable, other courts hold that successful litigation by definition cannot be a sham, and still other courts of appeals sometimes consider certain meritorious litigation to be a sham).

173. *See id.* at 60–61 (establishing the two-prong test).

174. *Id.* at 60.

reasonably expect the petition to be successful on its merits.[175] Then, if a court somehow finds an administrative review petition to be objectively baseless, it could apply the second prong and assess the petitioners' subjective motivations to use the administrative review to harm foreign competitors.[176] It would be difficult to show that an AD administrative review petition is objectively baseless because it is difficult to predict the outcome of an administrative review; thus, it would be difficult to prove that a petitioner could not expect at least a reasonable chance of success.[177]

Though the first prong makes it difficult for post-order settlement agreements to escape Noerr-Pennington immunity, some courts show movement away from a strict application of the sham exception test by incorporating an abuse of process analysis in Noerr-Pennington decisions, potentially making it easier to overcome Noerr-Pennington immunity.[178] Applying Justice Stevens's reasoning in *Professional Real Estate Investors*, the sham exception's first prong test of objective reasonableness might not be appropriate for determining whether the domestic parties should be subjected to antitrust liability because it is too difficult to effectively apply the first prong in complicated abuse of process situations.[179] In *Grip-Pak*, Judge Posner similarly distinguished the applicability of Noerr-Pennington immunity in abuse of process situations, arguing that Noerr-Pennington immunity is applied too broadly in abuse of process cases.[180] Though some question the two-prong sham exception test, courts are yet to collectively move away from this two-prong analysis and its objective baselessness requirement.[181] Thus, the sham exception would likely be ineffective in

175. *Id.*

176. *Id.* at 60–61.

177. *Cf.* Pierce & DeFrancesco, *supra* note 1 (explaining that the lengthy review process, court appeals, and sampling practices contribute to the unpredictability of administrative reviews).

178. *See Prof'l Real Estate Investors, Inc.*, 508 U.S. 49, 67–76 (Stevens, J., concurring) (questioning the majority's strict two-prong test); *see also* Grip-Pak, Inc. v. Illinois Tool Works, 694 F.2d 466, 471–73 (7th Cir. 1983) (suggesting the use of an abuse of process analysis to give more consideration to anticompetitive purposes in sham situations).

179. *Prof'l Real Estate Investors, Inc.*, 508 U.S. at 74–76 (Stevens, J., concurring).

180. *See Grip-Pak, Inc.*, 694 F.2d at 471–73 (refusing to rule that the difficulty in distinguishing between lawful and unlawful anticompetitive purposes is so acute that any anticompetitive purpose with the smallest basis in law can never be actionable under the Noerr-Pennington doctrine).

181. *See Prof'l Real Estate Investors, Inc.*, 508 U.S. at 55 n.3 (1993) (observing the multiple approaches courts of appeals have taken in determining Noerr-Pennington immunity under its sham exception yet applying the two-prong analysis); Music Center S.N.C. Di Luciano Pisoni & Co. v. Prestini Musical Instruments Corp., 874 F. Supp. 543, 548–49 (E.D.N.Y. 1995) (maintaining the two prong analysis for the sham

AD cases.[182]

3. *The Chinese Furniture Case Raises Many of These Antitrust and Anti-Competition Concerns*

In the Chinese furniture case, the ITC recognized that the administrative review process led to annual settlements between domestic and Chinese producers.[183] However, Commerce and the ITC refused to do more than briefly comment on the settlements, leaving the question of their legality open-ended.[184] This lack of administrative attention, however, does not necessarily imply that these settlements do not create antitrust liability for the domestic producers.

The domestic furniture industry's efforts to compel settlement agreements through threats of costly administrative reviews seem to openly infringe upon antitrust laws. With respect to the Sherman Act, these settlements involve collusive agreements amongst multiple parties that directly affect market price and volume conditions by artificially skewing the assigned dumping rates and assuring an uninterrupted flow of LTFV Chinese furniture.[185] On the price side, these agreements create additional costs and distortions that can force foreign producers to raise prices.[186] On the volume side, because the size of the settlement payments are based on the value of each Chinese firm's imports, a system of perverse incentives causes domestic producers to encourage more Chinese furniture imports so they can demand higher settlement payments.[187] These perverse incentives

---

exception).

182. *See* Cho, *supra* note 5, at 361 (finding the sham exception to likely be ineffective in AD cases because of courts' narrow interpretation of the exception).

183. Chinese Furniture, *supra* note 2, at 16.

184. *See id.* at 17, n.106 (observing that the ITC is not charged with enforcing antitrust laws); Combs, *supra* note 61 (reporting that Commerce, after repeated inquiries, continues to deny knowledge of the settlement arrangements); Hagerty, *supra* note 2 (quoting a Commerce spokesperson who did not approve of the settlements but explained that Commerce lacked the appropriate authority to investigate such agreements).

185. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 1, 5–7 (describing how a subset of domestic producers worked together to create these settlement "schemes" that enabled a continuous and substantial flow of subject imports into the U.S. market and allowed subject Chinese producers to maintain low deposit rates); *see also* Combs, *supra* note 61 (describing how multiple international and domestic parties were involved in designing the settlements).

186. *See* Chinese Furniture, *supra* note 2, at 29 (Additional Views of Comm'r Daniel R. Pearson) (observing that the furniture settlements imposed higher costs on the AD process, in addition to the costs normally associated with AD investigations).

187. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 7 (describing the "perverse incentives" of the settlements and how they do not serve the purpose of AD laws). *But see* Chinese Furniture, *supra* note 2, at 29 n.1 (Additional

are important because the Noerr-Pennington doctrine does not protect actions used to achieve a purpose that legislation is intended to curtail,[188] which, in this case, is the influx of subject Chinese imports. Most courts, however, apply Noerr-Pennington immunity regardless of the petitioning party's subjective intent for bringing the petition.[189] Thus, the exception would be ineffective in these settlement disputes unless courts begin to interpret the sham exception less strictly and focus more on the petitioners' subjective intent.[190]

These settlement agreements further restrain trade by treating some Chinese producers differently than others, depending on their relationships with domestic producers.[191] This abuse and restraint of trade carries over into the domestic furniture industry's exploitation of the administrative review process.[192] AD orders are intended to protect U.S. producers by limiting the volume of subject imports, but, because of these settlements, domestic furniture producers were able to manipulate market quantities and encourage the importation of subject Chinese furniture so they could line their pockets with more settlement cash.[193]

Views of Commissioner Daniel R. Pearson) (noting that the record did not indicate a clear connection between the settlements and the volume of subject imports).

188. California Motor Transp. Co. v. Trucking Unlimited, 404 U.S. 508, 515 (1972).

189. *See* Assoc. Container Transp. Ltd. v. United States, 705 F.2d 53, 58–59 (2d Cir. 1983) (considering petitioning parties' subjective motivations to be irrelevant for Noerr-Pennington purposes). *See generally* Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc., 508 U.S. 49 (1993) (holding that the Noerr-Pennington sham exception does not turn on subjective intent, but instead turns on objective reasonableness).

190. *Compare* Cho, *supra* note 5, at 361 (observing that AD petitions would likely be protected from antitrust liability by courts' strict sham exception analyses), *with* Grip-Pak, Inc. v. Illinois Tool Works, Inc., 694 F.2d 466, 471–72 (7th Cir. 1982) (applying abuse of process reasoning to a sham exception analysis so as to focus more on the petitioners' subjective intent).

191. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 63 (suggesting that some Chinese furniture firms may receive different settlement terms because of their commercial relationships with domestic firms); Hagerty, *supra* note 2 (finding potential for abuse when settlements permit U.S. furniture producers to treat Chinese producers differently because Chinese producers with more favorable settlement terms could gain an unfair advantage in the U.S. market); *see also* Posthearing Brief of Guandong Yihua Timber Industry Co., *supra* note 127, at 2 (explaining that AD laws and regulations fail to consider that settlement fees can vary depending on the commercial relationship between a foreign and domestic firm).

192. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 3–4 (describing domestic petitioners' use of the petitioning process as a "shakedown" of as many Chinese producers as possible).

193. *See* Prehearing Brief of Guangdong Yihua Timber Industry Co., Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203, at 11 (Dec. 2010) (Review); Wooden Bedroom Furniture from China, Inv. No. 731-TA-1058, USITC Pub. 4203, at 29 (Dec. 2010) (Review) (contrasting the purpose of AD laws

4. *These Settlement Agreements Severely Frustrate the Object and Purpose of U.S. Trade Laws*

The primary purpose of AD orders is to protect domestic industries from unfairly priced imports being dumped into the U.S. market.[194] However, when private parties agree to post-order settlement agreements without any agency oversight, the AD orders no longer serve the purpose of the AD laws.[195] Instead of limiting the flow of subject foreign imports, these settlements actually encourage the opposite outcome by tying the size of settlement payments to subject import volumes.[196]

Moreover, AD laws specifically describe certain distinct types of AD settlements, but these private post-order agreements do not qualify as any of those statutorily authorized settlement methods.[197] Plus, through these settlement agreements, domestic producers manage to circumvent Congress's intent by retrieving duty revenues from the cash settlement payments.[198]

III. BY ACCOUNTING FOR POST-ORDER SETTLEMENT AGREEMENTS, THE FUNCTIONAL PURPOSE OF AD LAWS CAN BE RESTORED

This Section describes several methods by which AD laws can change to properly account for the existence of private post-order settlement agreements. Above all, the function and purpose of U.S. AD laws need to be restored so that domestic industries can effectively compete without the threat of unfairly dumped goods.[199]

---

with the effects of the settlements).

194. *E.g.*, Schnerre, *supra* note 7.

195. *See* Chinese Furniture, *supra* note 2, at 29 (Additional Views of Commissioner Daniel R. Pearson) (believing that the settlement agreements did nothing to limit the harmful effects of subject imports).

196. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 7 (arguing that the domestic producers' use of settlement agreements to both encourage subject imports and turn a profit violates the purpose of AD laws); *see also* Chinese Furniture, *supra* note 2, at 29 (Additional Views of Commissioner Daniel R. Pearson) (explaining how these settlement agreements do not benefit the domestic industry or economy).

197. KAYE & DUNN, *supra* note 9; Macrory, *supra* note 8, at 24–26.

198. *See* Lester, *supra* note 4 (observing that, with the repeal of the Byrd Amendment, Congress did not intend for U.S. producers to receive AD duty payments, but they still manage to do so through these settlement agreements).

199. *See* Chinese Furniture, *supra* note 2, at 29 (Additional Views of Commissioner Daniel R. Pearson) (elucidating how these settlement agreements do not provide the domestic benefits that AD orders are designed, but not necessarily required, to encourage); Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 7 (arguing that AD settlements incentivize unfairly priced imports).

A. Recommendation 1: Expressly Prohibit Private Post-Order Cash Settlement Agreements Under AD Law

AD laws could be amended to expressly limit the available settlement methods for AD cases and prohibit private post-order settlement agreements.[200] If private post-order settlements are expressly prohibited, then administrative reviews would still be available, but they could not act a means of coercing foreign industries into settlement agreements.

A domestic interested party's withdrawal of a petition for administrative review could signal Commerce to investigate whether the withdrawal was related to a settlement agreement. Commerce and the ITC are well-positioned to investigate any potential post-order settlements because they have extensive access to domestic industry information via the questionnaires they send to domestic producers.[201] Commerce and the ITC's questionnaires could ask domestic firms if they are party to, or otherwise aware of, any private settlement agreements. Moreover, both Commerce and the ITC have broad powers to investigate domestic industries' business data, so they would be well-positioned to notice suspicious petition withdrawals.[202] Under this method, private post-order settlement agreements would violate AD laws; therefore, antitrust concerns and Noerr-Pennington immunity would not be as important.[203]

If Recommendation 1 were applied in the Chinese furniture case, once the domestic interested parties withdrew their petitions for an administrative review, Commerce would begin investigating whether any domestic firms were involved in any settlement agreements with foreign producers as part of the administrative review process.[204] Commerce would then refuse to acknowledge any withdrawals of petitions for review that were related to collusive settlement agreements and would proceed with those administrative reviews.

---

200. *Cf.* KAYE & DUNN, *supra* note 9 (describing private, non-statutory methods of settling AD administrative reviews); Macrory, *supra* note 8, at 24–26 (listing the methods for settling AD cases and administrative reviews under AD laws).

201. *See* Cho, *supra* note 5, at 395 (clarifying that these questionnaires are not optional and that the ITC and Commerce can investigate further to verify the questionnaire responses).

202. *See* Schnerre, *supra* note 7, at 497.

203. *Cf.* Combs, *supra* note 61 (admitting that Commerce and the ITC cannot investigate antitrust violations because of jurisdiction restrictions, but they can both investigate AD issues).

204. *Cf.* Schnerre, *supra* note 7, at 497 (noting that Commerce and the ITC already have "powerful" administrative and investigative powers).

B. Recommendation 2: Give Commerce and the ITC Greater Oversight Over How the Settlements Proceed

Because the administrative review process generates costly uncertainty for both domestic and foreign producers, there are benefits to settling and avoiding this uncertainty;[205] to preserve these benefits, Congress could change AD laws to create a standardized mechanism for settling post-order AD agreements. By providing strict agency oversight over the settlement process, the agencies can ensure the agreements do not frustrate the purpose of AD laws. The statutory provisions for suspension agreements could act as a model because they already require Commerce to determine whether settlements are in the public interest before approving the agreements.[206]

Agency oversight may also correct the perverse incentives created by the unregulated private post-order agreements and refocus the purpose on limiting subject imports.[207] Questionnaires could again identify the relevant domestic and foreign producers and ensure that all interested parties included in the settlement receive equal or similar settlement terms.[208]

In applying Recommendation 2, the agreements between domestic and Chinese furniture producers would be subjected to strict agency oversight. Before any settlement could be reached, Commerce would have to investigate the agreement to ensure that its effects would be in the interests of the public and the domestic industry. If the settlements do not to serve those interests, Commerce would not allow a withdrawal of the petitions and would proceed with the administrative review.

C. Recommendation 3: Change the Retrospective Nature of AD Duty Assessments

It is the retrospective liability determinations' inherent uncertainty that

205. KAYE & DUNN, *supra* note 9.

206. 19 U.S.C. § 1673c(a)–(c); Schnerre, *supra* note 7, at 503.

207. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 7 (arguing that the unregulated settlements incentivize subject imports); KAYE & DUNN, *supra* note 9 (explaining that since these settlement agreements occur without any agency oversight, neither the settlement process nor its terms are subject to agency approval or public interest analysis).

208. *See* Posthearing Brief of Furniture Retailers of America, *supra* note 128, at 63 (suggesting that Chinese furniture firms receive different settlement terms because of their commercial relationships with domestic firms); Hagerty, *supra* note 2 (observing that Chinese producers with more favorable settlement terms could gain an unfair advantage in the U.S. market).

encourages post-order settlement agreements.[209] Therefore, if the retrospective liability determination is removed, or at least reformed, the parties will not be incentivized to circumvent statutory mechanisms. However, the initial duty rates should not act as permanent rates for the life of the AD order because that would enable foreign firms to freely increase their dumping margins after an order is assigned. To avoid this, AD duties should be adjusted through the administrative review process, but there should be a limit as to how much the duty liability can change every year, i.e., allow the new duty rates to fluctuate only by a certain percentage in either direction, year-over-year.[210] This will prevent subject foreign producers from raising their dumping margins after an order is implemented, and it will reduce the foreign producers' uncertainty about their future liability.

Under Recommendation 3, Chinese producers would have had less incentive to agree to the domestic producers' terms because they would not have faced such costly uncertainty about future liability.[211] Therefore, the agreements may not have transpired in the first place, but if they had, and either Recommendation 1 or Recommendation 2 was also in place, it would ease the investigative burden on Commerce and the ITC because fewer Chinese producers would likely settle.

CONCLUSION

This is a case where the overlap between two distinct, yet related, areas of the law does not increase the laws' respective utilities; instead, the overlap allows private actors to circumvent both. Though post-order AD settlement agreements precisely fit the description of the types of collusive and anticompetitive behavior that antitrust laws are designed to prevent, the procedures and processes of trade laws make them permissible. Likewise, these settlement agreements frustrate the object and purpose of AD laws, but exceptions to antitrust laws prevent that frustration from being mitigated.

Under current antitrust and AD laws, these settlement agreements are likely legal because of the protection afforded by the Noerr-Pennington doctrine and courts' narrow application of its sham exception. Unless

209. *See infra* Section II.A.

210. *Cf.* Pierce & DeFrancesco, *supra* note 1 (arguing that the lack of a "cap" on foreign producers' exposure to AD duty liability under the administrative review system increases the relative cost of the uncertainty faced by those foreign producers subject to review).

211. *See* Ikenson, *supra* note 47 (reporting that domestic furniture producers effectively enhanced threats of heightened uncertainty and higher duties by requesting reviews of Chinese firms with relatively low AD duties).

courts make a concerted effort to incorporate an abuse of process analysis into Noerr-Pennington decisions, these settlements will continue until the AD laws are changed. If the laws are not changed, domestic industries will continue extorting their foreign competitors and lining their pockets with cash, all while encouraging the very same unfair imports that AD laws are supposed to curtail.

IGNORING THE TECHNICALITY'S TEMPTATION: INTERPRETING THE CITIZENSHIP OF A FOREIGN OFFICIAL UNDER THE FOREIGN CORRUPT PRACTICES ACT

ELIZABETH GRANT*

The Foreign Corrupt Practices Act ("FCPA") prohibits bribing "foreign officials," but it does not define the word "foreign" or give any guidance to what citizenship the official must have to fall under the FCPA. Adding to the difficulty when defining "foreign," the recent rise in prosecutions and increased FCPA case law has failed to produce an obvious answer as to how a court should address these issues. This makes it harder for businesses to comply with the FCPA or, in the alternative, obtain favorable deferred prosecution agreements. This Comment argues that, while the FCPA excludes those with U.S. citizenship from being "foreign officials" to protect defendants from an ambiguous criminal statute, businesses should structure compliance programs to treat "foreign officials" as including those with U.S. citizenship. Section I of this Comment traces the evolution of the United States' anti-bribery obligations. Section II analyzes courts' divergent readings of the FCPA and the problem this creates for interpreting whether "foreign" implies that the actor must be a non-U.S. citizen to constitute a "foreign official." Section III identifies how a court would use past approaches to interpret the term "foreign" to include

* Staff Member, *American University Business Law Review*, Volume 2; J.D. Candidate, *American University, Washington College of Law*, 2014; B.A. in English, *The University of Pennsylvania*, 2011. I would first like to thank my editors, Yuki Haraguchi and Art Howson, and the entire *American University Business Law Review* staff for their work in editing this piece for publication. I would also like to thank my faculty advisor, Professor Amy Tenney, for her wonderful advice and dedication to the piece, and Professor Stephen Vladeck for his constant encouragement from the idea's beginning. Most importantly, a special thank you to my family, especially my mother, for their unwavering love and support, without whom this would not be possible.

actors with U.S. citizenship, but ultimately would adopt a defendant's narrow definition under the rule of lenity. It then argues that businesses should consider this loophole nonexistent for compliance program purposes. The Conclusion places this issue within the current debate over narrowing the FCPA's terms, determining that it shows the need for statutory clarification and reform to better allow businesses to comply with the law.

INTRODUCTION

On paper, the United States criminalizes bribing "foreign officials,"[1] but despite clear evidence, some instances of bribery have escaped prosecution.[2] In June 2012, R. Allen Stanford stood trial for running an investment fraud scheme.[3] At trial, a witness recounted that Stanford bribed an Antiguan bank regulator, Leroy King, as part of his actions to

1. 15 U.S.C. § 78dd-1 (2012).

2. *See, e.g.*, Richard L. Cassin, *Stanford's Antigua Bribes: Why No FCPA Charges*, THE FCPA BLOG (June 15, 2012), http://www.fcpablog.com/blog/2012/6/15/stanfords-antigua-bribes-why-no-fcpa-charges.html (noting that the government did not pursue FCPA charges against Allen Stanford though there was clear testimony of bribery at his trial).

3. *See id.* (explaining that Stanford stood trial for charges of fraud and conspiracy for fake certificates of deposit sold to investors); *see also* Press Release, Dep't of Justice, Allen Stanford Sentenced to 110 Years in Prison for Orchestrating $7 Billion Investment Fraud Scheme (June 14, 2012) *available at*, http://www.justice.gov/opa/pr/2012/June/12-crm-756.html.

support the Ponzi scheme.[4] Although King may have qualified under the Foreign Corrupt Practices Act ("FCPA") as a "foreign official" because he was an instrumentality of another state, U.S. officials chose not to charge Stanford with a FCPA violation.[5] Richard Cassin, a FCPA expert, inferred that Stanford escaped charges because King maintained dual citizenship with the United States and Antigua and Barbuda, West Indies.[6]

This situation presents particular difficulty for businesses that operate overseas because unpredictable application of the FCPA hinders compliance with the law.[7] The Stanford case could indicate relaxed FCPA enforcement by the United States,[8] or it could mean that the United States interprets the FCPA's "foreign official" to mean a non-U.S. citizen.[9] Although a business could operate under the assumption that the United States interprets "foreign official" to include only non-U.S. citizens, the business would do so at the risk of preparing an inadequate compliance program and potentially violating the statute.[10]

When looking for a citizenship requirement, there is little tangible legal guidance for businesses to follow.[11] The FCPA specifically criminalizes the bribery of "foreign officials," making it unlawful for a business and its

---

4. *See* Cassin, *supra* note 2 (recounting testimony that Stanford bribed Antiguan bank regulators with a Swiss slush fund to keep his Ponzi scheme afloat).

5. *See id.*

6. *See id.* (conjecturing that the federal government withheld charges due, in part, to the potential for costly appeals over the question of whether a "foreign official" is a non-citizen when the "foreign official" had dual U.S. citizenship). The government may also have been deterred from filing charges because Stanford already faced fraud and conspiracy charges that carried lengthy prison terms. *Id.*

7. *See* Catherine Dunn, *Compliance Hinges on the Tricky Definition of 'Foreign Official,'* LAW.COM (Aug. 27, 2012), http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202568942016&FCPA_Compliance_Hinges_on_the_Tricky_Definition_of_Foreign_Official (noting the importance of clear statutory terms, which enable businesses to create effective compliance programs and follow business practices that lead to fewer violations).

8. *See* Cassin, *supra* note 2 (noting that the Department of Justice ("DOJ") chose not to bring charges against Stanford in the face of clear indication of bribery).

9. *See id.* (proposing that the DOJ withheld charges against Stanford because of a lack of authority and case law supporting that a "foreign official" includes a U.S. citizen).

10. *See* Dunn, *supra* note 7 (explaining that businesses need clarity to create effective and comprehensive compliance programs); Dep't of Justice Criminal Div. & SEC Enforcement Div., *A Resource Guide to the Foreign Corrupt Practices Act*, DEP'T OF JUSTICE (Nov. 14, 2012), at 71 http://www.justice.gov/criminal/fraud/fcpa/guide.pdf (stating that robust compliance programs help employees avoid FCPA violations and help obtain non-prosecution agreements, or deferred prosecution agreements from the DOJ and the Securities and Exchange Commission ("SEC"), potentially reducing fines and punishment for the business).

11. *See* Cassin, *supra* note 2 (noting the lack of precedent to suggest that the term "foreign official" includes U.S. citizens and the uncertainty it created for the DOJ).

agents to offer payment, promise to pay, or authorize the payment of anything of value to any foreign official or foreign political party.[12] Additionally, the payments must be made for purposes of influencing any act or decision of the official or political party to obtain or retain business of the payor.[13] The statute defines "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof" without specifically defining "foreign" to mean a non-U.S. citizen.[14] While cases have analyzed the meaning of other aspects of the statutory definition of "foreign official,"[15] courts have yet to decide on the specific citizenship requirements of a "foreign official," leaving businesses without a concrete answer as to what constitutes a FCPA violation.[16] These business are left with high-stakes guesswork as to whether a court would decide that "foreign official" under the FCPA implies that the actor be a non-U.S. citizen.[17]

This Comment argues that the FCPA contains a loophole that excludes those with U.S. citizenship from being considered "foreign officials" to protect the defendant from statutory ambiguity, but that businesses should structure compliance programs to treat the term "foreign officials" as including those with U.S. citizenship. Section I traces the evolution of the United States' anti-bribery commitments. Section II analyzes courts' divergent readings of the FCPA and the problem it creates in determining whether "foreign" implies that the actor must be a non-U.S. citizen to constitute a "foreign official." Section III identifies how a court could use past approaches to interpret the term "foreign" to include actors with U.S. citizenship, but ultimately concludes that courts should follow the rule of lenity—a method of statutory interpretation that reads ambiguous criminal statutes in favor of defendants. It then argues that businesses should ignore this interpretation for compliance program purposes. Finally, this Comment places this issue in the context of the present debate over whether to narrow the FCPA's terms, concluding that statutory clarity is needed to better allow businesses to comply with the statute.

---

12. 15 U.S.C. § 78dd-1(a) ("It shall be unlawful . . . [to] influenc[e] any act or decision of [a] foreign official in his official capacity, (ii) induc[e] [a] foreign official to do or omit to do any act in violation of the lawful duty of such official, or (iii) secur[e] any improper advantage . . . .").

13. *Id.* ("[The payment must be made] to assist such issuer in obtaining or retaining business for or with, or directing business to, any person . . . .").

14. *Id.* § 78dd-1(f)(1)(A).

15. *See, e.g.*, United States v. Aguilar, 783 F. Supp. 2d 1108, 1115 (C.D. Cal. 2011) (interpreting the "instrumentality" prong of "foreign official").

16. *See* Cassin, *supra* note 2 (noting that a court has never faced an instance where the "foreign official" in question had citizenship other than that of another country).

17. *See* Dunn, *supra* note 7 (describing the risks to businesses caused by ineffective compliance programs).

I. THE EVOLUTION OF THE UNITED STATES' ANTI-BRIBERY OBLIGATIONS AND RECENT COURT DECISIONS THAT HAVE INTERPRETED THE FCPA

This Section sets out the United States' domestic and international anti-bribery obligations, and then reviews recent case law interpreting the FCPA as a means to understanding the different possible ways to approach the interpretation of "foreign."

A. The United States' Domestic Anti-Bribery Obligations

The United States enacted the FCPA in 1977 to combat bribery.[18] The FCPA does not cover all types of commercial bribery, but rather prohibits the bribery of "foreign officials," foreign political parties, and candidates for a foreign political party.[19] Specifically, the FCPA defines "foreign officials" to include officers and agents of a foreign government or that government's agency, department, or instrumentality.

Substantively, the FCPA criminalizes active bribery as opposed to passive bribery—meaning that it is illegal to give actively a bribe, but legal to receive a bribe.[20] The FCPA covers parties who issue certain classes of securities, and it includes the issuer's "officer, director, employee, or agent."[21] The FCPA prohibits a covered party, its employees, or agents from offering, paying, promising to pay, or authorizing payment of money, gift, or anything of value to a "foreign official" or political party.[22] Additionally, successful prosecution under the FCPA requires a showing that the bribes are intended to either influence an entity or induce an entity to (1) use its influence to secure an improper advantage, (2) violate its lawful duty, or (3) influence its decisions made in an official capacity.[23]

Over the years, the FCPA has evolved to meet various cultural and international attitude shifts in determining what behavior is acceptable.[24]

---

18. *See* S. REP. No. 95-114, at 3–4 (1977) (Conf. Rep) (noting that the FCPA was enacted to combat foreign bribery, partly in response to domestic and foreign bribery incidents that exposed the U.S. companies engaging in widespread bribery, and partly in response to a growing moral imperative to level the playing field in international business by attacking bribery overseas).

19. 15 U.S.C. § 78dd-1(a)(1)–(3).

20. *See generally id.* § 78dd-1 (addressing the bribe giver, rather than the bribe receiver who acts as a statutory element as the "foreign official").

21. *Id.* § 78dd-1(g)(1).

22. *Id.*

23. *See id.* § 78dd-1(a)(1)-(3).

24. *See* Eric J. Smith, Comment, *Resolving Ambiguity in the FCPA Through Compliance with the OECD Convention on Bribery of Foreign Public Officials*, 27 MD. J. INT'L L. 377, 392–93 (2012) (explaining that amendments made to the FCPA were in response to the United States' international obligations under the Organisation for Economic Co-operation and Development's Anti-Bribery Convention).

Congress enacted the FCPA in 1977 as a response to unethical corporate behavior, particularly the SEC's Watergate-era investigations and discovery of corporate slush funds used to bribe foreign government officials for favorable business procurement.[25] Congress deemed criminalizing this behavior necessary to stopping the unethical conduct that tarnished the image of American businesses abroad and to restore integrity and public confidence to the American business system.[26]

Congress amended the FCPA twice since its enactment.[27] The 1988 amendment, part of the Omnibus Trade and Competitiveness Act, changed the FCPA in two major ways.[28] First, Congress altered the scienter requirement for third-party bribes.[29] Second, Congress clarified the facilitation payments exception,[30] while adding two more defenses corporations could use to protect themselves against liability.[31] Congress intended these changes to lessen the obstacles on exports faced by U.S. companies, while "attempting to balance a resolute opposition to global corporate bribery with the promotion of U.S. economic interests abroad."[32] Congress next amended the FCPA in 1998 to comply with the United States' obligations under the Organisation for Economic Co-Operation and Development's ("OECD") Convention Combating Bribery of Foreign

25. *See* Pete J. Georgis, Comment, *Settling with Your Hands Tied: Why Judicial Intervention Is Needed to Curb an Expanding Interpretation of the Foreign Corrupt Practices Act*, 42 GOLDEN GATE U. L. REV. 243, 248–49 (2012) (positing that the FCPA was enacted in response to corporations' rampant unethical conduct as discovered during the Watergate era's SEC and Internal Revenue Service ("IRS") investigations that uncovered corporate slush funds used to gain overseas business agreements).

26. *See id.* at 250 (quoting then Treasury Secretary W. Michael Blumenthal) ("Many U.S. firms have taken a strong stand against paying foreign bribes and are still able to compete in international trade. Unfortunately, the reputation and image of all U.S. businessmen has been tarnished by the activities of a sizeable number, but by no means a majority of American firms. A strong anti-bribery law is urgently needed to bring these corrupt practices to a halt and to restore public confidence in the integrity of the American business system.").

27. *See* Smith, *supra* note 24, at 383–85.

28. *See* Georgis, *supra* note 25, at 252–53 (explaining that the Omnibus Trade and Competitiveness Act clarified and amended the 1977 terms to promote U.S. economic interests abroad in the wake of a growing trade deficit).

29. *See* Smith, *supra* note 24, at 381 (acknowledging that the FCPA criminalizes bribes only if the bribe giver has knowledge that the payments are made for bribing purposes).

30. *See* Georgis, *supra* note 25, at 253–54 (noting that the FCPA clarified facilitation payments to include " 'routine governmental action,' " like clerical duties).

31. *See id.* (noting that the Act permitted defenses of "reasonable and bona fide expenditures," and "legality in the host country").

32. *See id.* at 254 (relaying the Act's reasoning, as stated in the congressional findings, that corporations' concerns about the FCPA's scope should not eclipse the FCPA's original intention).

Public Officials in International Business Transactions and Related Documents ("OECD Anti-Bribery Convention").[33] In this amendment Congress broadened the "foreign official" definition to include the language "any person."[34]

B. *The United States' International Anti-Bribery Obligations*

In addition to its domestic obligations, the United States has become party to international conventions that impose anti-bribery obligations.[35] As one of the first pieces of anti-bribery legislation, the FCPA stands as a model for much of the subsequent international anti-bribery conventions, with each convention reflecting different cultural norms and anti-bribery goals.[36]

1. *OECD Convention Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents*

The United States signed the OECD Anti-Bribery Convention as part of one of the first internationally binding efforts to combat bribery.[37] The text mirrors the FCPA and outlaws bribing foreign public officials.[38] This Convention does not include all countries, but rather the OECD member

33. *See id.* at 254–55 (noting the United States' obligations to conform its domestic legislation with the OECD Anti-Bribery Convention's provisions, including broadening "bribery," and the FCPA's jurisdictional scope).

34. *See* Smith, *supra* note 24, at 381 n.25 (explaining that the term "foreign official" needed new language to clarify and conform with the OECD Anti-Bribery Convention's broader scope).

35. *See Steps Taken to Implement and Enforce the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions – United States*, ORG. FOR ECON. CO-OPERATION AND DEV. 2 (May 31, 2011), http://www.oecd.org/daf/briberyininternationalbusiness/anti-briberyconvention /42103833.pdf [hereinafter *OECD*] (listing three international bribery conventions that the United States has joined).

36. *See* Michael B. Bixby, *The Lion Awakens: The Foreign Corrupt Practices Act—1977 to 2010*, 12 SAN DIEGO INT'L L.J. 89, 98–100 (2010) (describing how the United States has taken a leadership role in its domestic legislation and in leading international efforts to combat bribery as a founding member of the OECD and as a proponent of the OECD Anti-Bribery Convention).

37. *See OECD*, *supra* note 35, at 1 (noting the United States' date of instrument ratification and acceptance as December 8, 1998).

38. *Compare id.* (explaining that the FCPA is the United States' implementing legislation), *and* 15 U.S.C. § 78dd-1(f)(1)(A) (outlawing the bribing of "foreign officials"), *with Convention Combating Bribery of Foreign Public Official in International Business Transactions and Related Documents*, ORG. FOR ECON. CO-OPERATION AND DEV. 7 (2011), http://www.oecd.org/dataoecd/4/18/38028044.pdf [hereinafter *OECD Convention*] (requiring a member country to criminalize a person who intentionally offers, promises, or gives any undue advantage to a "foreign public official" in order to gain an improper business advantage through the action or inaction of the "foreign public official").

countries and any other countries that have joined the OECD Working Group on Bribery in International Business Transactions ("Working Group").[39] The OECD Anti-Bribery Convention requires its parties to enact domestic legislation and monitors countries' compliance as its enforcement mechanism.[40] Despite this seemingly relaxed enforcement procedure, the Working Group brings the parties together and successfully relies on the power of peer monitoring to ensure compliance with the document's requirements.[41] Thus, the United States has a strong incentive to comply with the document, especially because it is a founding member of the OECD.[42] Further, the Working Group reports on each country's implementation of legislation, efforts to combat bribery of foreign public officials, and compliance with the OECD Anti-Bribery Convention.[43]

2. United Nations Convention Against Corruption

Additionally, the United States is party to the United Nations Convention Against Corruption ("U.N. Corruption Convention").[44] This represents the largest international effort to combat corruption.[45] The text recognizes the harm corruption causes to the growth of democracy, the rule of law, and sustainable development of countries.[46] The U.N. Corruption Convention also deals with general forms of corruption, not limiting itself to business corruption.[47] As such, the U.N. Corruption Convention requires that parties

39. *See OECD Convention*, *supra* note 38, at 13, 19 (listing the member countries of the OECD Anti-Bribery Convention and providing that non-member countries may become parties by joining the Working Group).

40. *See id.* at 7, 11 (mandating that parties take measures to enact domestic legislation and requiring that the parties monitor their success to ensure full implementation).

41. *See id.* at 18–19 (providing for monitoring and follow-up procedures that include regular reviews, self-evaluation, and mutual evaluation and examination of specific issues concerning bribery in international business).

42. *See* Smith, *supra* note 24, at 396 (discussing how acceptance between the members and the recognition of a shared responsibility to combat bribery may have elevated the OECD Anti-Bribery Convention to the level of customary international law).

43. *See OECD Convention*, *supra* note 38, at 18–19 (requiring reports to objectively assess countries' progress in implementing the OECD Anti-Bribery Convention as a part of monitoring efforts). *See generally OECD*, *supra* note 35 (demonstrating an example of a country analysis report for the United States).

44. *See OECD*, *supra* note 35, at 2.

45. *See generally* United Nations Convention Against Corruption, Oct. 31, 2003, T.I.A.S. No. 06-1129, 2349 U.N.T.S. 41 (providing the list of parties as one hundred and sixty-one countries and the European Union).

46. *See id.* at 1, 2349 U.N.T.S. at 145.

47. *See id.* at 3, 5, 2349 U.N.T.S. at 146, 148 (emphasizing that the purpose is to prevent and fight corruption on a macro level and calling for preventative measures to address corruption broadly).

implement domestic measures in the areas of prevention, criminalization and law enforcement, international cooperation, and asset recovery.[48]

3. Inter-American Convention Against Corruption

The United States has also signed the Inter-American Convention Against Corruption ("IACAN").[49] IACAN was the first international agreement to address corruption.[50] The parties to IACAN are the member countries of the Organization of American States.[51] The agreement requires that member states cooperate for the eradication of corruption in the performance of public functions.[52] To achieve these aims and ensure compliance, IACAN calls for oversight mechanisms that rely on individual monitoring assessment and member state support.[53]

4. Agreement Establishing the Group of States Against Corruption

While not a member of the European Council, the United States signed the Agreement Establishing the Group of States Against Corruption ("GRECO") in 1998.[54] This group includes the European Council's member states and observer states.[55] The agreement covers methods of strengthening the member countries' capacity to monitor and evaluate anti-corruption measures.[56] The agreement is enforced through follow-up assessment and mutual evaluation to ensure compliance.[57]

---

48. *See id.* at 5–6, 2349 U.N.T.S. at 148.

49. *See OECD*, *supra* note 35, at 2.

50. *See* Inter-American Convention Against Corruption, March 29, 1996, S. TREATY DOC. No. 105-39 (1998), at 1, 35 I.L.M. 724, 724 (1996) (noting the adoption date as 1996 and the entry date as 1997).

51. *See id.* at 3–5, 35 I.L.M. at 728–29 (defining the scope of the convention as corruption that effects state parties).

52. *See id.* at 11, 35 I.L.M. at 732 (asking parties to provide mutual assistance to carry out the recommendations and calling for member states to strengthen mechanisms to prevent, detect, eradicate, and punish corruption).

53. *See id.* at 3–4, 35 I.L.M. at 728 (emphasizing the reliance on individual monitoring and mutual support as the force used to ensure compliance, rather than the creation of penalties under IACAN).

54. *See OECD*, *supra* note 35, at 2 (listing the United States as an observer state to the Group of States Against Corruption and a signing party to GRECO).

55. *See* Comm. of Ministers, *Resolution (98)7*, COUNCIL OF EUR. (May 5, 1998) http://www.coe.int/t/dghl/monitoring/greco/documents/resolution(99)5_en.asp (listing forty-seven member states, which include six observer states and the European Council).

56. *See id.*

57. *See id.*

C. The United States' Obligations in Practice and Recent Court Decisions

In the past ten years, the U.S. government has increased its prosecution of FCPA violations.[58] This trend reflects a shift in enforcement priorities that have changed as cultural norms have shifted both domestically, to more actively enforce existing legislation, and internationally, to increase anti-corruption efforts.[59] However, while the global marketplace has changed, the United States continues to affix antiquated terms to modern business practices, which creates ambiguity in those terms' application to changed business practices.[60] The combination of increased prosecutions, evolving business structures, and ambiguous terminology is reflected in recent business case law.[61]

1. United States v. Kay

The United States Court of Appeals for the Fifth Circuit indicated that bribing a government official to reduce sales taxes and customs duties for a business entity could be illegal because it possibly falls within the "obtaining and retaining business" language of the FCPA.[62] In 2001, the United States charged Douglas Murphy and David Kay, president and vice president of American Rice, Inc., with FCPA violations after the company made improper payments to Haitian officials to lower the company's sales taxes and customs duties in Haiti.[63] In response, the defendants moved to dismiss the charges against them, arguing that the United States failed to state a claim because the payments fell outside the FCPA's scope.[64] The court considered whether the payments made to reduce taxes and duties fell

58. *See* Mike Koehler, *The Foreign Corrupt Practices Act in the Ultimate Year of Its Decade of Resurgence*, 43 IND. L. REV. 389, 389 (2010) (announcing 2009 as the ultimate year of the FCPA's resurgence, emerging from a decade of enforcement after having been rarely enforced).

59. *See id.* at 415 (analyzing the United States' increased enforcement as a product of the need to keep pace with changing norms).

60. *See id.* at 410 (arguing that the application of "foreign official" to state-owned enterprises should be challenged in court for lack of judicial scrutiny).

61. *See id.* at 410–12 (listing enforcement actions that involve an issue with "foreign official" and highlighting the rise of case law).

62. *See* United States v. Kay, 359 F.3d 738, 756 (5th Cir. 2004) (defining the scope of the FCPA to include tax savings in the event that the bribe was intended to produce an effect to aid in "obtaining or retaining business").

63. *See id.* at 740–42.

64. *See* United States v. Kay, 200 F. Supp. 2d 681, 682 (S.D. Tex. 2002) (noting that the defendants argued that the FCPA's plain language does not prohibit the payments at issue, that the legislative history favors a narrow interpretation of the acts the FCPA intends to prohibit, that the rule of lenity resolves ambiguities in favor of the defendants, and that the FCPA does not give fair warning that the conduct at issue is illegal).

within the FCPA's requirement that payments made to "foreign officials" must be for the purpose of obtaining or retaining business.[65] The United States District Court for the Southern District of Texas granted the defendant's motion to dismiss and found that, as a matter of law, payments made to obtain favorable tax treatment are not payments to obtain or retain business.[66] On appeal, the Fifth Circuit reviewed the issue, reversed the district court, and concluded that payments made to "foreign officials" to evade unlawfully sales tax and customs duties fell within the FCPA's scope.[67] The court clarified that, to prove a FCPA violation, there must be a showing of intent that unlawful payments directed to foreign officials to reduce taxes and duties would actually improve the company's business.[68]

2. United States v. Aguilar

In *United States v. Aguilar*, the United States District Court for the Central District of California ruled that the term "instrumentality" under "foreign official" could include an employee of a state-owned enterprise, depending on the entity's characteristics.[69] The United States charged Keith Lindsey, Steve Lee, and Lindsey Manufacturing Co. with FCPA violations concerning payments made to a government-controlled electric utility company.[70] The defendants moved to dismiss on the grounds that under the FCPA, an employee of a state-owned corporation cannot be deemed a "foreign official."[71] The court denied the motion and found the electric utility company had attributes that made it an "instrumentality" under the FCPA, making the employees that received the bribes "foreign officials" for the purposes of a FCPA violation.[72]

---

65. *See id.* (explaining the issue before the court as ruling on the defendant's motion to dismiss).

66. *See id.* at 686 (concluding that Congress considered and rejected language to broaden the FCPA's scope to cover the conduct at issue and thus determined that the indictment's allegations did not fall under the FCPA).

67. *See Kay*, 359 F.3d at 756 (finding that the conduct could fall within the scope of the FCPA and that the case should not be dismissed because the conduct did not fall outside the scope as a matter of law).

68. *See id.*

69. *See* United States v. Aguilar, 783 F. Supp. 2d 1108, 1115 (C.D. Cal. 2011) (ruling that the term could include at least some state-owned enterprises and listing characteristics that would tend to place an entity under the definition).

70. *See id.* at 1109–11 (alleging that the defendants paid high-ranking employees of an electric utility company controlled by the Mexican government in order to gain an unlawful business advantage).

71. *See id.* at 1110 (asserting that the government's wholly-owned subsidiary was neither an "agency," "department," nor "instrumentality" of a foreign government).

72. *See id.* at 1116–17 (concluding that not all government wholly-owned subsidiaries are excluded from "instrumentality," and, after a fact-based examination, dismissing the defendant's motion to dismiss).

3. United States v. Carson

United States v. Carson held that "instrumentality" under "foreign official" can include an employee of a state-owned enterprise.[73] In the case, the United States indicted three named defendants for charges of FCPA violations concerning payments made to foreign, state-owned companies on behalf of their employer, Controlled Components Inc., for the purpose of obtaining or retaining business.[74] The defendants moved to dismiss the charges on grounds that the United States failed to state an offense, arguing that employees of state-owned companies never constitute "foreign officials" under the FCPA.[75] The court denied the defendants' motion and concluded after a statutory analysis that some business entities, including state-owned companies, could, on a case-by-case basis, be "foreign officials" under the "instrumentality" category.[76]

II. THE DIVERGENT APPROACHES OF FCPA STATUTORY INTERPRETATION CREATE PROBLEMS FOR COURTS ATTEMPTING TO INTERPRET "FOREIGN"

This Section analyzes the previously presented obligations and case law to demonstrate that prior instances of FCPA statutory interpretation fail to produce an obvious result as to how a court would interpret the term "foreign."

A. Prior FCPA Statutory Treatment Has Produced Differing Interpretation Approaches for FCPA Terms and Leaves Uncertain As to How a Court Would Interpret "Foreign"

This first Section analyzes the different modes of reasoning that courts have used in past interpretations, showing there is no established way that a court would interpret "foreign." To date, courts have interpreted "obtain and retain business" and "foreign official" by reading the terms

73. *See* United States v. Carson, No. SACR 09 00077 JVS, 2011 WL 5101701, at *8 (C.D. Cal. May 18, 2011) (concluding that "instrumentality" could include some business entities depending on the entity's nature and characteristics).

74. *See id.* at *1–2 (indicting the defendants for nearly five million dollars worth of bribes made on behalf of their employer, Controlled Components Inc., to various foreign, state-owned companies).

75. *See id.* (contending that state-owned companies are never "departments," "agencies," or "instrumentalities" of a foreign government and therefore could not meet the definition of "foreign official" under the FCPA).

76. *See id.* at *3–6, *8 (employing an ordinary reading of the term and considering the term in light of both the surrounding terms and the statute as a whole to reject the defendant's assertion as impermissibly narrowing the FCPA and ultimately concluding that the state-owned business could be an "instrumentality" on a fact-based analysis).

expansively.[77] In addition, courts have varied their modes of interpretation when reading the same term.[78] There are six approaches courts have used to interpret the FCPA.

1. A Court Will Start with Plain Language Readings of FCPA Terms

When interpreting a statute, a court will first look to the text for a definition.[79] If a term is not defined in the statute, the court will consider the plain and unambiguous meaning of the language as controlling.[80] Courts interpreting the FCPA start their inquiry with this mode of interpretation.[81] Generally, FCPA statutory language interpreted by a plain language reading favors broad definitions.[82]

In *Kay*, the Fifth Circuit attempted to employ a statutory interpretation of "obtaining or retaining business" by looking to the FCPA's language, but found it provided little guidance.[83] The FCPA fails to provide what constitutes "business" under the statute's prohibition of bribes paid to "obtaining or retaining business," and the court needed to articulate a scope to rule on the case's issues.[84] Without a given statutory definition, the court looked to the plain meaning of "obtaining or retaining business" for guidance.[85] In analyzing the parties' proposed dictionary definitions, the court found that each party asserted different meanings to the term, making the plain language reading debatable.[86]

Additionally in *Aguilar*, the court needed to interpret "instrumentality"

77. *See* Amy Deen Westbrook, *Enthusiastic Enforcement, Informal Legislation: The Unruly Expansion of the Foreign Corrupt Practices Act*, 45 GA. L. REV. 489, 530–32 (2011) (arguing that the terms under the FCPA are being reexamined and have been enforced expansively, which has created problems).

78. *See id.* (citing instances where courts have approached "foreign official" in different manners).

79. *See, e.g.*, United States v. Kay, 359 F.3d 738, 742–43 (5th Cir. 2004) (commencing the statutory interpretation with plain language reading).

80. *See, e.g., id.* (explaining the mode of interpretation used when a statute fails to provide a definition for a term).

81. *See, e.g., id.* (employing the plain language reading as the first step of its interpretation of "obtaining or retaining business").

82. *See, e.g., id.* at 744 (refusing to determine conclusively the meaning of "obtaining or retaining business" with just the plain language meaning).

83. *See id.* at 743 (analyzing the language "obtaining or retaining business" to see if the language could encompass payments made to reduce taxes).

84. *See id.* at 743–44 (finding that the statute does not provide a defined scope of "business," meaning the court needed to interpret "business" through other modes of statutory interpretation to find whether the term encompassed bribes paid to custom officials).

85. *See id.* at 744.

86. *See id.* (concluding that each proposed definition could apply plausibly to the statute).

in the statutory definition of "foreign official."[87] The court noted that the FCPA did not supply a definition, and as such, the court looked to see if a plain language reading existed that would control the meaning.[88] The court adopted the defendant's definition, providing that an "instrumentality" could never encompass a state-owned enterprise.[89] The adoption allowed the court to avoid a full inquiry and recognize that the varying proposed definitions would not provide an unambiguous definition and that "instrumentality" would be better defined with the words surrounding it.[90]

Furthermore in *Carson*, the court started its interpretation of "instrumentality" by giving the term its ordinary meaning, but determined that plain meaning interpretation provided little help.[91] The court used dictionary definitions to gather both commonplace and legal definitions.[92] To further its argument that state-owned enterprises are included under the "instrumentality," the United States asserted a broad definition that the defendants rejected.[93] The defendants asserted that the United States' broad definition would render the proceeding terms in the statute meaningless and further pushed the court to accept that there was no settled legal definition of "instrumentality."[94]

As the reviewed dictionary definitions did not provide an unambiguous definition, the court accepted the defendant's argument and turned to other means to determine the term's meaning.[95]

---

87. *See* United States v. Aguilar, 783 F. Supp 2d 1108, 1113–14 (C.D. Cal. 2011) (addressing the defendant's claims that a wholly state-owned corporation could never comprise a "foreign official" under "instrumentality").

88. *See id.* at 1113 (looking first at the statute's language to see if a given definition could address the defendants' argument, then continuing to read the term according to its plain meaning in the absence of a statutory definition).

89. *See id.* at 1113–14 (acknowledging the varying definitions of such a broad noun).

90. *See id.* (acknowledging that the definitions of "instrumentality" range from acting as an agency or means for implementation, to a subsidiary branch through which policies and functions are carried out).

91. *See* United States v. Carson, No. SACR 09 00077-JVS, 2011 WL 5101701, at *4 (C.D. Cal. May 18, 2011).

92. *See id.* at *4 (using Black's Law Dictionary, Oxford English Dictionary, and Webster's New Dictionary to gather a variety of definitions).

93. *See id.* at *3–4 (explaining that the United States argued that state-owned enterprises are included under either "agencies" or "instrumentalities" of the state as opposed to the defendants, who argued that under the statute's given definition, employees of state-owned companies can never be foreign officials).

94. *See id.* at *5 (discussing the defendants' argument against adopting a narrow reading that would render "agency" or "department" merely superfluous language in the statute).

95. *See id.* (accepting the defendant's proposal to further consider the term in the context of its preceding terms as opposed to accepting the United States' broad interpretation without further inquiry).

2. *A Court Will Most Likely Read FCPA Terms Within the Context of the Preceding Terms and in View of the FCPA As a Whole*

After a plain language reading, a court may interpret the statutory language in accordance with the statute's policy and objective and in a way that each term within the statute has an operative effect.[96] Overall, courts interjected common sense and logic to establish terms' scopes when reading the FCPA according to this principle, but resisted relying solely on this method to establish a definitive meaning.[97]

In *Kay*, the court looked to determine the scope of "obtain or retain business" and found that "assist" suggested a broader scope of "obtain or retain," but failed to concretely establish the actual scope.[98] Additionally, the court declared that the remainder of the statutory language did not clearly suggest that the business nexus element should be construed broadly or narrowly.[99] Lastly, the court looked at the FCPA's title to find that it suggested a broader interpretation.[100] Ultimately, the court found arguments for both broad and narrow readings supported by other statutory language and concluded that there was not a persuasive argument to establish the phrase's scope.[101]

Additionally, in *Carson*, the court looked to interpret "instrumentality" in the context of "agency" and "department," and within the FCPA as a whole.[102] The court first noted that "instrumentality" refers to an entity that carries out governmental functions, but is also intended to capture entities that are not "agencies" or "departments."[103] In looking to interpret the term as it would be in the vernacular, the court declared that "instrumentality"

---

96. *See, e.g.*, United States v. Kay, 359 F.3d 738, 742 (5th Cir. 2004) (looking to the FCPA's policy to determine the scope of "obtaining or retaining business").

97. *See, e.g.*, *Carson*, 2011 WL 5101701, at *5 (employing a common logic-based analysis to determine the meaning of "instrumentality").

98. *See Kay*, 359 F.3d at 744–45 (deciding that the scope of "obtain or retain business" inconclusively lies somewhere between a broad interpretation and the defendant's asserted narrow reading, potentially covering the actions described in the case).

99. *See id.* at 745 (finding that the language in the "facilitating payments" exception, and the section addressing the award of new business, both offered plausible arguments for the United States and the defendants).

100. *See id.* (interpreting the title to suggest a broader reading of the terms, but finding that it fails to establish concretely a broad reading with such a generic title).

101. *See id.* at 745–46 (concluding that the statute's language does not establish a definite scope and could support a narrow or broad interpretation).

102. *See Carson*, 2011 WL 5101701, at *5 (moving the statutory interpretation beyond a plain language reading of "instrumentality" to consider it in conjunction with its surrounding terms in the FCPA).

103. *See id.* (giving "instrumentality" the same generalized definition as the two preceding terms, but ultimately differentiating its specific meaning).

would function like an "agency" or "department" through which the government conducts business without excluding a state-owned entity.[104] Furthermore, the court rejected the defendant's argument that "instrumentality" should only consist of entities that share the same characteristics as an "agency" and "department" because doing so would narrow the FCPA when it was intended to attack broadly government corruption.[105]

In *Aguilar*, the court used this principle to look at "department" and "agency" to create a list of characteristics of an "instrumentality."[106] Although the defendants argued that "instrumentality" could only encompass entities that shared characteristics of both "departments" and "agencies," the court disagreed.[107] The court dismissed this logic because sharing the characteristics of the two proceeding terms would render "instrumentality" surplus statutory language.[108] Unlike *Carson*, which looked to define "instrumentality" as capturing the entities not covered by "agency" and "department," *Aguilar* pointed to some shared characteristics that offer guidance as to what constitutes "instrumentality" and proposed a guiding list of features.[109]

3. *A Court Will Seldom Look to Other Statutes to Aid FCPA Term Interpretation*

When possible, a court may look to other statutes that contain the disputed term as a means of interpretation.[110] Courts interpreting the FCPA

104. *See id.* at *5 (reasoning similarly to the court in McBoyle v. United States, 283 U.S. 25, 51 (1931), where the court interpreted "vehicle" by asking what the word evoked in the common mind).

105. *See id.* at *5 (using the statutory intent to read "instrumentality" in light of the FCPA as a whole).

106. *See* United States v. Aguilar, 783 F. Supp. 2d 1108, 1114–15 (C.D. Cal. 2011) (responding to and accepting the defendant's argument that the court should look to similarities between "agency" and "department" to define "instrumentality," as they are entities that possess some shared characteristics).

107. *See id.* at 1115 (finding a flaw in the defendant's logic by revealing that a state-owned corporation will never be an "instrumentality" under the defendant's definition because those entities do not always necessarily share the attributes of "agencies" and "departments").

108. *See id.* (noting that if the term must share all of the other two term's characteristics, it would rob "instrumentality" of its independent meaning and violate the canon of construction that advises against reading terms to void them of meaning).

109. *See id.* (providing a non-exclusive list of factors including: the entity provides a service to the citizens, government officials appoint key officers or directors, the government finances, at least in large, part the entity through funds through governmental appropriations or revenue raising activities, the entity is granted and exercises power to exercise its functions, and the entity is widely understood to perform official functions).

110. *See, e.g.*, *Carson*, 2011 WL 5101701, at *7 (offering the FSIA as an example

hesitate to make direct comparisons between different statutes, but still analyze parties' claims that employ this mode to glean congressional intent.[111] For example, the defendants in *Carson* argued that the court should look to the Foreign Sovereign Immunities Act's ("FSIA") definition of "foreign official."[112] The defendants asserted that because the FSIA deliberately included state-owned enterprises in its definition of "instrumentality," Congress therefore did not intend to include state-owned enterprises within "foreign official" when it failed to list it expressly under the FCPA.[113] The court found little merit in that argument, limiting its analysis to terms within the same statute.[114] Rather, the court noted that because Congress included state-owned enterprises under the FSIA's definition a year before they passed the FCPA, Congress might have intended to include state-owned enterprises under the FCPA.[115]

4. *A Court May Employ the* Charming Betsy *Canon of Construction to Aid in the Interpretation of the FCPA*

Courts may employ other canons of construction to suggest a statutory term's meaning in light of other legal doctrines, such as the *Charming Betsy* canon of construction. The *Charming Betsy*[116] canon states that statutes should not be construed to violate the law of nations or an international agreement to which the United States is a party.[117] Although one court has used this method, it did so in an authoritatively and conclusive manner, giving force to this method in future interpretations.[118]

---

which defines "instrumentality" and presenting it as persuasive evidence).

111. *See, e.g., id.* (refusing to apply the FSIA definitions to the FCPA definitions).

112. *See id.* (directing the court to the FSIA and asserting that Congress would have included state-owned enterprises in the "instrumentality" definition if it had intended to capture these entities under "foreign official").

113. *See id.* (relying misguidedly on the canon of construction *expressio unius est exclusio alterius*—"the express mention of one thing excludes all others"—to compare two different statutes instead of applying the canon of construction to one statute).

114. *See id.* (correcting the defendant's misguided argument by noting that the canon only has force when the items are in an associated group as to allow for an inference that excluded items were done so by choice).

115. *See id.*

116. Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804) (requiring that, when possible, a United States statute should be construed so that its interpretation does not violate international law or conflict with a United States international agreement).

117. *See* United States v. Aguilar, 783 F. Supp. 2d 1108, 1116 (C.D. Cal. 2011) (applying the *Charming Betsy* canon of construction and reasoning that if the United States is to receive benefits of international obligations, it should honor its international agreements).

118. *See, e.g., id.* at 1118 (applying definitively the OECD Anti-Bribery Convention to aid in the FCPA's interpretation).

In *Aguilar*, the United States argued that "instrumentality" should be read in light of the United States' treaty obligations that require the criminalization of bribes to officials in state-owned enterprises.[119] The court found that Congress specifically amended the FCPA in 1998 to implement the OECD Anti-Bribery Convention and therefore accepted the United States' argument that the FCPA should be read specifically to align with that treaty.[120] Moreover, because Congress amended only "foreign official," the court saw the amendment as supporting the United States' argument that "instrumentality" could include state-owned enterprises, despite not having added "state-owned corporations" to the FCPA.[121] Therefore, the court found that the FCPA should be construed according to the United States' obligations under the OECD Anti-Bribery Convention.[122]

5. *A Court May Review the Legislative History to Aid in the Interpretation of the FCPA*

When interpreting statutory ambiguity, a court may consult the legislative history to aid interpretation.[123] In FCPA interpretation cases, courts have decided to consult and ignore legislative history to clarify ambiguity.[124] Overall, courts have differed in applying this mode of interpretation, but when using it, tend to employ it as a backdrop to interpreting other terms.[125] For example, the *Aguilar* court turned to

119. *See id.* at 1116–17 (reviewing the 1998 Amendments that changed the FCPA in response to the United States' new obligations under the OECD Anti-Bribery Convention and arguing that the term should be read in light of that convention).

120. *See id.* (applying the *Charming Betsy* canon to the term "instrumentality" and the OECD Anti-Bribery Convention).

121. *See id.* at 1117–18 (finding that the OECD Anti-Bribery Convention reflects that Congress viewed "foreign official" as already encompassing state-owned corporations because Congress did not amend "instrumentality" or "foreign official" to conform with the Convention's definition of "foreign public official," which included broadly defined public enterprises).

122. *See id.* (reasoning, in part, that "instrumentality" could include state-owned corporations under the United States' obligations to the OECD).

123. *See id.* at 1117 (citing Levi Strauss & Co. v. Abercrombie & Fitch Trading Co., 633 F.3d 1158, 1171 (9th Cir. 2011)) (permitting a review of the legislative history if there is ambiguity in the language of the statute).

124. *See id.* (employing a legislative history review, but finding it unnecessary to base the ruling on the review); United States v. Kay, 200 F. Supp. 2d 681, 684–85 (S.D. Tex. 2002) (applying the legislative history to illuminate the term's scope). *But see* United States v. Carson, No. SACR 09-00077-JVS, 2011 WL 5101701, at *8 (C.D. Cal. May 18, 2011) (declining to pursue further statutory inquiry by analyzing the legislative history).

125. *See, e.g.*, *Aguilar*, 783 F. Supp. 2d at 1117, 1119 (deducing that the FCPA's legislative history lacked sufficient weight to establish conclusively the term's meaning).

legislative history to determine if Congress had intended to include state-owned corporations as an "instrumentality" under "foreign official."[126] After weighing arguments over whether the term included or excluded state-owned enterprises, the court concluded that the legislative history was inconclusive.[127] In response, the court circulated a hypothetical to the parties, ultimately deeming from the answers that Congress would not have viewed the specific case beyond the FCPA's reach just because the official was a state-owned corporation.[128]

In contrast to *Aguilar*, the court in *Carson* found it unnecessary to review the legislative history to determine the definition of "instrumentality."[129] The court argued that a review of legislative history is only necessary when the statutory language is ambiguous and within an incoherent statutory scheme.[130] As the court had already determined that "instrumentality" was unambiguous and within a consistent and coherent scheme, the court declined to address the parties' legislative history arguments.[131]

In *Kay*, the district court looked to the legislative history to determine the scope of "obtain or retain business."[132] The court consulted the 1977, 1988, and 1998 committee reports.[133] From this inquiry, the court found that Congress declined to amend the "obtain or retain" language to broaden the original definition's scope in both 1988 and 1998.[134] As such, the 95th Congress's intent controls when determining the language's scope.[135] With this in mind, the court determined that the payments made to reduce taxes and customs duties fell outside of the scope of "obtain or retain business"

126. *See id.* at 1117–18 (looking to the 1976 Senate bill, the 1977 House and Senate bills, and the 1988 and 1998 amendments to help clarify the definition).

127. *See id.* at 1119.

128. *See id.* at 1119–20 (proposing a hypothetical corporation and bribery incident, asking each side to apply its arguments to the new set of facts, and ultimately concluding that Congress would not have wanted to exclude the bribery from the FCPA's scope on a language technicality).

129. *See Carson*, 2011 WL 5101701, at *8.

130. *See id.* (citing Schindler Elevator Corp. v. United States, 131 S. Ct. 1885 (2011)).

131. *See id.* (declaring that previous determinations are sufficient for understanding "instrumentality" without looking further to the legislative history).

132. *See* United States v. Kay, 200 F. Supp. 2d 681, 683–84 (S.D. Tex. 2002) (continuing the statutory inquiry with a review of the legislative history after failing to concretely establish a definition by looking at the term's language).

133. *See id.* at 683–87 (listing the potential instances that Congress may have considered the term's language and gathering reports from each time Congress wrote or amended the FCPA).

134. *See id.* at 685–87 (reasoning that by declining to amend the term, the later Congresses accepted the 95th Congress's scope).

135. *See id.* at 686–87 (narrowing the range of pertinent legislative history to the time when Congress actively debated the term).

because Congress had rejected proposed bills that would have expressly broadened the FCPA's prohibited activities.[136]

6. A Court May Consider Applying the Rule of Lenity

When addressing statutory ambiguity, the defendant may argue that the court should apply the statutory construction, rule of lenity, to interpret the term in favor of the defendant if doubts about the meaning remain.[137] A court will interpret a term like this when the term's meaning proves so questionable to protect defendants who could have fairly believed their asserted definition.[138] Generally, courts have resisted applying the rule of lenity to the FCPA, as they had previously found its terms to have more than one plausible definition.[139] In *Kay*, the district court declined to apply the rule of lenity because it determined that the statue was not ambiguous.[140] If there was no ambiguity, the court determined that there was no reason to interpret the statute in the defendant's favor to avoid unfairness.[141] In *Carson*, the court declined to apply the rule of lenity because it did not find that there were two equally plausible and applicable definitions of the term "instrumentality."[142]

B. Prior FCPA Statutory Treatment Fails to Produce an Obvious Resolution as Applied to the Term "Foreign"

This Section applies the different modes of interpretation to the term "foreign" to establish citizenship requirements. The FCPA is ambiguous because the plain meaning of the word "foreign" conflicts with the definition of the word "official," which broadly refers to "any officer or employee."[143] A court could adopt the plain language meaning of "foreign," narrowly construing the term to exclude U.S. citizens from constituting "foreign officials" under the FCPA.[144] Conversely, a court

136. *See id.* at 684 (applying the legislative history to illuminate the term's scope).

137. *See id.* at 686–87.

138. *See id.* (explaining that the rule of lenity applies to protect a defendant from a lack of fair warning of a term's meaning).

139. *See id.* at 686–87.

140. *See id.* (finding that the statutory scheme clearly allows for facilitation payments).

141. *See id.* (resisting the rule's application because the defendant could fairly interpret "obtain or retain business").

142. *See* United States v. Carson, No. SACR 09-00077-JVS, 2011 WL 5101701, at *5 (C.D. Cal. May 18, 2011) (construing the rule of lenity narrowly to apply to instances of true statutory ambiguity).

143. 15 U.S.C. § 78dd-1(f)(1)(A).

144. *See* THE WOLTERS KLUWER BOUVIER LAW DICTIONARY 439 (Compact ed. 2011) ("a person or thing from a foreign country"). A narrow reading of the definition would interpret "foreign" as a person from another country, presumably excluding U.S.

could broadly construe the term's definition to include U.S. citizens under the word "any" provided in the statutory definition.[145] The use of court's past interpretation methods to interpret other FCPA terms creates varying results when applied to the interpretation of "foreign."

1. A Plain Language Reading Fails to Establish a Concrete Reading of "Foreign"

In instances of statutory interpretation, a court starts its inquiry with a term's plain and unambiguous statutory language.[146] As applied to "foreign official," the FCPA defines the term "foreign official," but does not provide a specific definition of "foreign" that references citizenship.[147]

Without a clear statutory definition, a court would give the term its ordinary plain language reading, taking into consideration the statute's policy objectives.[148] In past FCPA interpretation cases, courts have used both English language dictionaries and legal dictionaries to aid in the interpretation.[149] Definitions drawn from some English language dictionaries point to "foreign" as an adjective that describes a person or thing that belongs to another country.[150] Additionally, a review of major legal dictionaries offers similar differing definitions.[151] Neither set clarifies the definition, failing to establish concretely a coherent reading of "foreign."[152]

---

citizens.

145. *See generally* 15 U.S.C. § 78dd-1 (focusing on "any officer or employee" to interpret "foreign official" broadly).

146. *See, e.g.*, United States v. Kay, 359 F.3d 738, 742 (5th Cir. 2004) (commencing its interpretation inquiry by looking at the given language in the statute for a definition or meaning).

147. *See* 15 U.S.C. § 78dd-1(f)(1)(A) (defining the term "foreign official" as "any officer or employee of a foreign government," without definitively answering whether the "foreign official," as a person, must be non-U.S. citizen).

148. *Cf. Kay*, 359 F.3d at 742 (continuing the statutory interpretation by looking at the plain language reading and taking into account the statute's policy objective in response to the FCPA's failure to define the business nexus's scope).

149. *See id.* at 744 (citing Webster's Encyclopedic Unabridged Dictionary); United States v. Aguilar, 783 F. Supp. 2d 1108, 1113 (C.D. Cal. 2011) (citing Black's Law Dictionary).

150. *See, e.g.*, MERRIAM-WEBSTER COLLEGIATE DICTIONARY 490 (11th ed. 2007) (offering definitions ranging from "not being within the jurisdiction of a political unit" and "situated outside a place or country" to "born in, belonging to, or characteristic of some place or country other than the one under consideration").

151. *Compare* BLACK'S LAW DICTIONARY 719–20 (9th ed. 2009) ("of or relating to another country"), *with* THE WOLTERS KLUWER BOUVIER LAW DICTIONARY 439 (Compact ed. 2011) ("a person or thing from a foreign country"), *and* BARRON'S LAW DICTIONARY 223 (6th ed. 2010) ("belonging to another country or nation").

152. *Cf. Kay*, 359 F.3d at 744–46.

The plain language reading of the term "foreign" is ambiguous as used in "foreign official."[153] A court would declare the term ambiguous because the term can be read both expansively to include all people that meet the required elements of the "foreign official" definition, and narrowly to exclude those that meet the elements, but have U.S. citizenship.[154] Additionally, after consulting the dictionary definitions under a plain language reading, a court would find that the definitions fail to establish concretely that a "foreign official" implies that the person must be a non-U.S. citizen.[155] The varying definitions are similar to the definitions in *Kay*, where the plausible definitions varied too much in scope to assign definitively one to the term.[156] As the court in *Kay* found an ambiguous definition, a court would find that "foreign" is still ambiguous after a plain language reading.[157]

2. *"Foreign," Read in the Context of the Proceeding Language and the FCPA as a Whole, Does Not Conclusively Establish a Definition of "Foreign"*

A court would find that when looking to preceding terms and in view of the FCPA as a whole, the readings offer arguments for both an expansive and narrow view of "foreign."[158] First, "foreign" must be read in accordance with "official," much like the term "instrumentality" was read according to "department" and "agency" in the *Aguilar* case.[159] When

153. *Cf. Aguilar*, 783 F. Supp at 1113–15 (establishing the plain language reading was inconclusive for "foreign official"); *Kay*, 359 F.3d at 742 (finding the plain language reading insufficient for "obtaining or retaining business").

154. *See* 15 U.S.C.A § 78dd-1(f)(1)(A) ("any officer or employee" allows for a broad interpretation); *id.* § 78dd-1(a)(1)(A)(i) ("*foreign* official" allows for a much narrower interpretation) (emphasis added).

155. *See, e.g.*, MERRIAM-WEBSTER COLLEGIATE DICTIONARY 490 (listing multiple plausible definitions that can each alter the statutory meaning of "foreign" to either "not being within the jurisdiction of a political unit" or "born in, belonging to, or characteristic of some place or country other than the one under consideration").

156. *Compare Kay*, 359 F.3d at 744 (declaring the definition of "business" as a volume of trade and the purchasing or sale of goods in order to make a profit as too broad to assume a concrete definition), *with* BLACK'S LAW DICTIONARY 719–20 (9th ed. 2009) ("of or relating to another country"), *and* BARRON'S LAW DICTIONARY 223 (6th ed. 2010) ("belonging to another country or nation").

157. *Compare Aguilar*, 783 F. Supp. 2d at 1115–17 (finding the definitions differed to such an extent that the court adopted the defendant's definition for simplicity's sake to further analyze it using other interpretive means), *and Kay*, 359 F.3d at 742, *with* MERRIAM-WEBSTER COLLEGIATE DICTIONARY 490 ("not being within the jurisdiction of a political unit"), *and* THE WOLTERS KLUWER BOUVIER LAW DICTIONARY 439 (Compact ed. 2011) ("a person or thing from a foreign country").

158. *See Kay*, 359 F.3d at 742 (continuing its statutory inquiry of "to obtain or retain business" with the surrounding terms and in light of the FCPA's title and purpose).

159. *Cf. Aguilar*, 783 F. Supp. at 1113–14 (reading "instrumentality" in light of the

reading "foreign" in relation to "official," it can be interpreted as either the person who is foreign or the position within the foreign government.[160] Similarly, the term's definition as a whole supports either "foreign official" as an individual or the person's official capacity.[161] However, the statute's description of prohibited conduct bolsters the assertion that the FCPA references the job position, rather than the individual.[162] Furthermore, the statute's title lends support for an expansive reading of "foreign official" in that the acts themselves are foreign, and not necessarily referring to the bribery of a non-U.S. citizen.[163]

Having established ambiguity, a court would read the term in light of the statute as a whole and in the context of the preceding term.[164] When reading within the definition's components, it refers to the "foreign official's" position within the foreign government, rather than the person's foreign nationality.[165] Furthermore, the FCPA's title suggests the broad nature of the statute and emphasizes the "Foreign Corrupt Practice," as opposed to bribery of non-U.S. citizens.[166] However, these arguments are less persuasive when a court looks to "foreign official"—the phrase that generally connotes a person of non-U.S. citizenship.[167] Therefore, a court could not establish with certainty that particular term's definition and would rather look to other canons of construction.[168]

---

two preceding words in the definition's series to find it supported both broad and narrow definitions).

160. *See* 15 U.S.C. § 78dd-1(f)(1)(A) (defining the term as "foreign official" without addressing the two words separately).

161. *See id.* (dictating that "foreign official" is "any officer or employee of a foreign government").

162. *See id.* § 78dd-1(a)(1)(A)(i) (prohibiting "influencing any act or decision of such foreign official in his official capacity").

163. *See id.* § 78dd-1 (suggesting a broad reading from the title "Foreign Corrupt Practices" as not referencing specific types of corruption, but rather broad forms).

164. *E.g.*, United States v. Kay, 359 F.3d 738, 742 (5th Cir. 2004) (progressing the inquiry past a declared ambiguous term to read it in light of the other terms and FCPA as a whole).

165. *See* 15 U.S.C. § 78dd-1(f)(1)(A) (reading as "any officer or employee of a foreign government," which suggests that the government position supersedes the actual person).

166. *See generally id.* § 78dd-1.

167. Examining the possible natural meaning of "foreign" could aid in determining the composition of "obtain or retain business." *Cf. Kay*, 359 F.3d at 742–43.

168. *Cf.* United States v. Aguilar, 783 F. Supp. 2d 1108, 1115–17 (C.D. Cal. 2011) (finding that the conflicting definitions and lack of support from other terms and the FCPA could not conclusively establish a concrete meaning and leading the court to try and interpret the meaning through other means).

3. *Other Statutes to Aid in the Interpretation of "Foreign" Fail to Apply to "Foreign Official" and Persuasively Address Citizenship*

Although the *Carson* court looked to the FSIA to aid in the interpretation of "instrumentality," a court would be unable to apply the same logic to "foreign official." Although the FSIA provides clear citizenship requirements under "foreign state,"[169] a court would not use "foreign state" to interpret "foreign official" because the canon of construction that infers meaning from statutory omissions does not apply to a term across two different statutes.[170] The court was reluctant in *Carson* to consider this argument, and a court interpreting "foreign" would likely not find the FSIA persuasive because the FSIA does not define "foreign official."[171]

4. *The* Charming Betsy *Canon of Construction Interprets "Foreign" Expansively to Include Those with U.S. Citizenship*

A court would also interpret "foreign" in light of the U.S. international anti-bribery obligations.[172] *Aguilar* used the canon of construction that the term should be interpreted in light of U.S. international obligations, and a court at first impression would also use that canon of construction.[173] Applying this canon to "foreign," an analysis in light of the OECD Anti-Bribery Convention is persuasive that the term should be read expansively, as was done in *Aguilar*.[174] However, the OECD does not specifically define any terms with reference to specific citizenships.[175] Analysis in light of the U.N. Corruption Convention, the Inter-American Convention against Corruption ("IACAC"), and GRECO are similarly persuasive.[176] Specifically, the U.N. Corruption Convention calls for broad corruption reduction efforts and would support the term to include U.S. citizens under

169. *See* 28 U.S.C. § 1603 (2012) (defining "foreign state" as an agency or instrumentality without U.S. citizenship).

170. *See Aguilar*, 783 F. Supp. 2d at 1116–17 (correcting the defendant's logic that the canon of construction applies to lists of terms within a single statute).

171. *Cf. id.* (declining to make inferences of congressional intent to purposefully exclude a term from a list when comparing two statutes).

172. *See id.* (applying the *Charming Betsy* cannon of construction to "instrumentality").

173. *See, e.g.*, *id.* (broadly reading "foreign official" to conform with the OECD Anti-Bribery Convention, a U.S. international obligation).

174. *Cf. id.* (reading the term to conform to the U.S. international obligations).

175. *See OECD Convention*, *supra* note 38, at 6–8 (urging countries to fight corruption in a broad sense and take steps necessary to eradicate it).

176. *See generally* Inter-American Convention Against Corruption, *supra* note 50 (asking countries to strengthen all anti-corruption efforts); Comm. of Ministers, *supra* note 55 (urging countries to strengthen all anti-corruption measures); United Nations Convention Against Corruption, *supra* note 45 (urging countries to fight corruption at all levels, recognizing the widespread harm that it causes).

"foreign official."[177] A court would not likely consider these binding authority, but rather persuasive texts when looking to the FCPA in light of U.S. international obligations.[178]

When applying the *Charming Betsy* canon of construction, a court would likely find that under the United States' international obligations, a person that meets the requirements of "foreign official" does not have to be a non-U.S. citizen.[179] The international obligations focus less on the actual nationalities and more on the destructive nature of bribery, suggesting the term's interpretation should reduce the bribery where possible and not exclude bribe receivers due to U.S. citizenship.[180] In the event that a court does not apply the OECD Anti-Bribery Convention, according to *Charming Betsy*, a court should look at the other international obligations.[181] The U.N. Bribery Convention would not likely allow this loophole on citizenship as it would be adverse to the rule of law and undermine the efforts to establish it.[182] Congress has not amended the FCPA since the OECD Anti-Bribery Convention, and it may not have changed the FCPA after becoming party to the U.N. Bribery Convention because it viewed terms as sufficient to enforce our international bribery obligations.[183] As such, the FCPA will be enforced as complying with the U.N. Bribery Convention, meaning that "foreign" should be interpreted broadly to encompass non-U.S. citizens.[184]

---

177. *See* United Nations Convention Against Corruption, *supra* note 45, at 27–28, 2349 U.N.T.S at 146 (imploring countries to take action to fight corruption on all levels and all types, presumably not supporting a citizenship exception).

178. *See* Inter-American Convention Against Corruption, *supra* note 50, at 8–10, 35 I.L.M 730–31 (asking countries to reduce corruption, while recognizing member state sovereignty in implementing the Convention).

179. *Cf. Aguilar*, 783 F. Supp. 2d at 1116–17 (expanding "foreign official" under the canon of construction to meet international obligations).

180. *See generally OECD Convention*, *supra* note 38 (taking a broad perspective on corruption fighting); United Nations Convention Against Corruption, *supra* note 45 (seeking corruption's eradication); Inter-American Convention Against Corruption, *supra* note 50 (recognizing corruption's destructive nature); Comm. of Ministers, *supra* note 55 (strengthening measures to combat corruption).

181. *See, e.g.*, *Aguilar*, 783 F. Supp. 2d at 1116–17 (applying *Charming Betsy* to interpret "instrumentality" in light of the OECD Anti-Bribery Convention).

182. *See* United Nations Convention Against Corruption, *supra* note 45, at 1–2, 2349 U.N.T.S. at 145 (stressing the establishment and strengthening of the rule of law by eradicating the undermining efforts of corruption and bribery).

183. *See* 15 U.S.C. § 78dd-1 (failing to provide a citizenship requirement after the 1998 Amendment updating "foreign official" to conform with the OECD Anti-Bribery Convention).

184. *See generally* United Nations Convention Against Corruption, *supra* note 45 (requiring parties to take *all* measures possible to eradicate corruption).

5. *A Review of the Legislative History Does Not Specifically Exclude Those with U.S. Citizenship Under "Foreign"*

A court would not find any significant additional means of interpretation in the 1988 or 1998 amendments.[185] A court would also not glean much from the legislative history of the 1977 FCPA.[186] Congress wrote the legislation to encompass foreign transactions, and in doing so, Congress generally implied business in a foreign country.[187] Additionally, the 1977 FCPA focused on what bribery did for the rule of law and democracy, not the terms in general.[188] Therefore, Congress may not have used the word "foreign" to address specifically non-U.S. citizens, but rather in an attempt to focus on the general bribery of foreign governments and their employees as a general category.[189] Without specifically amending "foreign official" to include a citizenship requirement, the legislative history does not conclusively establish one reading.[190]

Additionally, a court could take the approach that *Aguilar* took in deciding how Congress would have seen the facts in the instant case.[191] The *Aguilar* court also looked at "foreign official," and as such, a court would likely adopt the *Aguilar* court's approach and find that Congress would not have wanted the bribe to escape punishment because of a technicality in the language.[192] This means that a court interpreting "foreign" would similarly side with the *Aguilar* court and decide that when the official is a person that would otherwise meet the definition of "foreign official," it should not matter that the person has dual-citizenship.[193]

---

185. *See* Georgis, *supra* note 25, at 252–55 (explaining that the amendments addressed foreign public organization and facilitation payments).

186. *See id.* at 248–49 (noting that the 1977 FCPA debates focus strongly on Congress's intent to pass the law in order to protect our reputation overseas in bribing foreign governments).

187. *See id.* at 249–50 (recognizing that Congress intended to address bribery in a non-domestic sense)

188. *See id.* at 250 (stressing the United States' reputation in the global economy and seeing itself as a leader in promoting anti-corruption efforts globally).

189. *See id.* (looking to create the FCPA to address the issue of offering bribes overseas to corruptly obtain business advantages).

190. *See* United States v. Aguilar, 783 F. Supp. 2d at 1108, 1119 (C.D. Cal. 2011). (declining to use the legislative history in the term's analysis, as it was inconclusive on whether or not Congress intended to include state-owned enterprises under "foreign official").

191. *See id.* at 1116–19 (employing a congressional intent analysis after failing to establish from the legislative history that "foreign official" included state-owned enterprises).

192. *Cf. id.* at 1116–17 (illustrating the technicality that arises and gleaning that Congress would avoid such an outcome).

193. *Cf. id.* at 1119–20 (applying the court's proposed hypothetical to "foreign official" to find that a common sense reading was appropriate to interpret

When deciding whether to include the legislative history, a court would decide to review the history like the courts in *Aguilar* and *Kay*.[194] As such, a court would likely review the legislative history, but not give much weight to it.[195] In applying a similar hypothetical to the one the court proposed in *Aguilar*, a court would likely rule that Congress did not intend a dual-citizenship technicality to prevent the prosecution of a bribe, if the person was acting as an official of a foreign government.[196]

6. *An Application of the Rule of Lenity Construes "Foreign" in Favor of the Defendant*

The rule of lenity could compel a court to construe "foreign" in favor of the defendant.[197] The rule of lenity considers that if there are two equally plausible plain language readings of "foreign," a defendant might have fairly assumed that "foreign" implied non-U.S. citizen and acted accordingly.[198] A court might find that "foreign," after employing all other available modes of interpretation, supports two divergent definitions and leaves the court to guess as to what Congress intended.[199] Despite having never applied the rule of lenity to other FCPA terms, a court interpreting "foreign" could find it necessary to employ the rule because the narrow and broad readings are both equally plausible.[200] Therefore, the court could construe "foreign" narrowly as the defendants assert.[201]

"instrumentality").

194. *See id.* at 1116–17 (declining to apply a traditional legislative history interpretation of "instrumentality"); United States v. Kay, 359 F.3d 738, 743–44 (5th Cir. 2004) (deciding that the term "obtain or retain" was ambiguous and the statutory scheme incoherent regarding citizenship, therefore not looking to the legislative history).

195. *See id.* at 1119–20 (declining to look at legislative history); *accord Kay*, 359 F.3d at 749–50 (dismissing a legislative analysis).

196. *Cf. Aguilar*, 783 F. Supp. 2d at 1116–17 (surmising that Congress would not have meant for a language technicality to allow an instance of foreign bribery to go unprosecuted).

197. *See* United States v. Kay, 200 F. Supp. 2d 681, 686–87 (S.D. Tex. 2002) (defining the rule of lenity as construing language in favor of the defendant in instances where one must guess as to what Congress intended).

198. *See id.* (applying the rule of lenity only to instances when the term's meaning is unclear or when the defendant does not have fair warning of its meaning).

199. *Compare* BLACK'S LAW DICTIONARY 719–20 (9th ed. 2009) ("of or relating to another country"), *with* THE WOLTERS KLUWER BOUVIER LAW DICTIONARY 439 (Compact ed. 2011) ("a person or thing from a foreign country"), *and* BARRON'S LAW DICTIONARY 223 (6th ed. 2010) ("belonging to another country or nation").

200. *See generally supra* Section II (arguing and demonstrating that multiple interpretations of "foreign" are equally plausible to a defendant interpreting the FCPA and acting according to its terms).

201. *But cf.* United States v. Carson, No. SACR 09-00077-JVS, 2011 WL 5101701, at *9–10 (C.D. Cal. May 18, 2011) (construing the rule of lenity narrowly as applied to

III. A COURT'S INTERPRETATION OF "FOREIGN OFFICIAL" WOULD LIKELY CREATE A LOOPHOLE BY PROTECTING THE DEFENDANT FROM STATUTORY AMBIGUITY, BUT BUSINESSES SHOULD STRUCTURE COMPLIANCE PROGRAMS THAT TREAT "FOREIGN OFFICIALS" AS INCLUDING THOSE WITH U.S. CITIZENSHIP

A court should read the term "foreign official" expansively to include non-U.S. citizens, as the expansive reading reflects the FCPA's original goal of eradicating foreign bribery and fulfills the United States' international anti-bribery obligations.[202] However, a court could also apply the rule of lenity, creating a loophole and protecting defendants that bribe those "foreign officials" with U.S. citizenship.[203] Ultimately, when creating compliance programs, businesses should reconcile the uncertainty and consider "foreign official" to include those with U.S. citizenship to protect against the FCPA's ambiguity.[204]

A court would likely first declare "foreign official" an ambiguous term and employ a plain language reading and a subsequent reading in light of the surrounding terms, finding that both readings fail to concretely establish a definition due to plausible conflicting meanings.[205] As such, a court would continue its interpretation by consulting the terms of other statutes, but would not persuasively establish a citizenship definition of "foreign official" from the terms of the FSIA or any similar statutes.[206] However, a court reading the term in light of the legislative history and the United States' international obligations would likely establish that "foreign official" should not exclude U.S. citizens.[207]

Despite the reasons that a court should expansively read "foreign official," a court could very well apply the rule of lenity, requiring it to rule in favor of a defendant's argument for a narrow interpretation.[208] The rule's

---

"instrumentality" to apply only to instances of true statutory ambiguity).

202. *See* United States v. Aguilar, 783 F. Supp. 2d at 1108, 1116–17 (C.D. Cal. 2011) (applying *Charming Betsy* to interpret "instrumentality" and expand the term in light of the OECD Anti-Bribery Convention's broad notion of corruption).

203. *See Kay*, 200 F. Supp. 2d at 686–87 (defining the rule of lenity as being construed in favor of the defendant in instances where one must guess as to what Congress intended, thereby protecting the defendant and its conduct).

204. *See* Dunn, *supra* note 7 (finding that language clarification would provide greater confidence to bring violations of the FCPA in instances of foreign bribery, thereby enabling better compliance programs).

205. *See supra* Section II.

206. *See id.*

207. *See id.*

208. *See* United States v. Carson, No. SACR 09-00077-JVS, 2011 WL 5101701, at *9–10 (C.D. Cal. May 18, 2011) (withholding from applying the rule of lenity as applied to "instrumentality" because it was not an instance of true statutory ambiguity with two plausible definitions).

application could constrain a court from interpreting the FCPA to capture the few cases that profit from language technicalities and lack of clear definitions in the statute.[209] As such, this rule opens a loophole for defendant businesses to engage in foreign bribery under protection of statutory ambiguity and the rule of lenity.

This loophole creates difficulty for businesses when structuring compliance programs for overseas operations.[210] Without actual knowledge that a court would find both definitions of "foreign" equally plausible and then apply the rule of lenity for the defendant's benefit, businesses lack certainty that the "foreign official's" U.S. citizenship protects its conduct from what otherwise would trigger a FCPA violation.[211] Additionally, a court could possibly withhold the rule of lenity and expansively read the term, finding that the defendant business should have understood that "foreign official" implied any person working in the position's capacity.[212] Without a definitive indication of what a court would do, the loophole's temptation and uncertainty should be treated as effectively nonexistent for purposes of structuring an effective compliance program.

Further adding to the uncertainty, the DOJ and SEC continue to give no indication of whether either agency would bring a FCPA violation, and if so, how they would prosecute it in the event that a business engaged in bribery with a "foreign official" that had U.S. citizenship.[213] Although past actions might indicate that the DOJ is unlikely to bring such a case, businesses cannot safely create compliance programs assuming that the DOJ and SEC have acquiesced to such behavior.[214] The recent DOJ and SEC Prosecution Guide reflect the contrary, and suggest that the agencies will continue to aggressively enforce the FCPA.[215] This could very well include prosecuting instances where the "foreign official" has U.S.

209. *But cf.* United States v. Aguilar, 783 F. Supp. 2d at 1108, 1116–17 (C.D. Cal. 2011).

210. *See* Dunn, *supra* note 7 ("[H]aving the company and the enforcement agency back home agreeing on what those two words mean can be the difference between bribery and compliance.").

211. *See id.*

212. *See generally Carson*, 2011 WL 5101701 (finding that the defendant should have understood instrumentality to encompass state-owned enterprises and therefore not applying the rule of lenity).

213. *See generally* Dep't of Justice Crim. Div. & SEC Enforcement Div., *supra* note 10 (failing to address the citizenship of a "foreign official").

214. *See generally* Cassin, *supra* note 2 (discussing an instance where the DOJ may not have pursued a FCPA violation where the "foreign official" had dual U.S. citizenship).

215. *See generally* Dep't of Justice Crim. Div. & SEC Enforcement Div., *supra* note 10 (noting that the prosecutions would continue at the increased pace).

citizenship, and to effectively avoid enforcement actions, businesses should advise against it in compliance programs.[216]

The FCPA's continued uncertainty hinders business compliance programs. Until Congress fixes the loophole by amending the statute to include a definition of "foreign" to make it clear that "foreign official" may include a person with U.S. citizenship, businesses lack the necessary clarity they need to ensure compliance and should tailor their practices to err on the side of caution.[217]

CONCLUSION

The FCPA prohibits bribes to "foreign officials," but it does not define the word "foreign" or give guidance on what citizenship the official must have.[218] Adding to the difficulty, the recent rise of prosecution and case law fails to produce an obvious answer as to how a court would address the issue and rule on the citizenship of a "foreign official."[219] This presents challenges to businesses when creating effective compliance programs and exposes business to the risks of FCPA violations and less favorable deferred prosecution agreements.[220] However, amidst the confusion, on first impression a court would likely find that a person who meets all of the elements of a "foreign official," but who has U.S. citizenship, would still constitute a "foreign official," given recent court interpretations applied to "foreign." Despite this, in light of the rule of lenity and its recent applications, a court may be compelled to accept a defendant's argument for a narrow reading of the term "foreign."[221] This creates a loophole that further contributes to uncertainty and undermines the FCPA's goals.[222]

Never having reached a court, and lacking direct treatment from an authoritative source, this ambiguity creates uncertainties for businesses

---

216. *See* Bixby, *supra* note 36, at 98 (noting how the reach of "foreign official" was expanded to recognize the growth of state-owned enterprises).

217. *See* Dunn, *supra* note 7 (advocating for statutory language clarification to better create compliance programs).

218. *See* 15 U.S.C. § 78dd-1(f)(1)(A) (defining "foreign official" without mention of a citizenship requirement).

219. *See, e.g.*, United States v. Carson, No. SACR 09-00077-JVS, 2011 WL 5101701, at *10 (C.D. Cal. May 18, 2011) (interpreting "instrumentality," relying heavily on a language reading of the term).

220. *See* Dunn, *supra* note 7 (detailing the relationship between favorable treatment from the government in prosecution agreements and non-prosecution agreements for comprehensive compliance programs).

221. *But cf.* United States v. Kay, 200 F. Supp. 2d 681, 686–87 (S.D. Tex. 2002) (defining the rule of lenity as being construed in favor of the defendant in instances where one must speculate on congressional intent).

222. *See generally* Dunn, *supra* note 7 (asserting that the ambiguity can lead to unintentional violations and encourage intentional violations).

conducting operations overseas.[223] The issue is indicative of the growing debate in the United States over expanding the FCPA to include a more modern notion of anti-corruption in commercial transactions and reigning in the FCPA's expansion to return the legislation to its original narrow focus.[224] However, in the midst of this debate, the statute's terms do not reflect the modern realities of a global market place, creating situations that the original statute did not consider.[225] Until statutory reform directly addresses the ambiguity, businesses should err on the side of caution and operate with compliance programs that treat "foreign officials" as including those that meet the FCPA's elements and have U.S. citizenship.

223. *See id.* (arguing for the term's clarification to ensure more predictable enforcement actions).

224. *See* Westbrook, *supra* note 77 (comparing the FCPA to the UK Anti-Bribery Act and arguing that the FCPA could expand to include all commercial bribery).

225. *See, e.g.*, Koehler, *supra* note 58, at 410 (arguing that the application of "foreign official" to state-owned enterprises should be challenged in court for lack of judicial scrutiny).

NOTE

THE POLI-INTEL INDUSTRY: CONSIDERING THE COMMON LAW'S APPLICATION IN INSIDER TRADING UNDER THE STOCK ACT

ERNIE C. JOLLY*

President Barack Obama signed the Stop Trading on Congressional Knowledge Act ("STOCK Act") into law on April 4, 2012. Congressional silence on the STOCK Act's purview over the political intelligence industry and the lack of guidance from the Securities Exchange Commission ("SEC") have led practitioners and scholars to speculate on the STOCK Act's reach. Due to uncertainty, Congress should clarify its intent behind the STOCK Act, and the SEC should provide further guidance on the proper application of its securities laws while considering fundamental principles of fraud established through common law. Applying common law principles to political intelligence activity would weed out fraudulent behavior without having an overbroad impact, a risk enforcement officials run when applying vague insider trading principles to political intelligence activity. Ultimately, without further guidance, the STOCK Act's applicability to political intelligence activities will remain speculative,

* Staff member, *American University Business Law Review*, Volume 2; J.D. Candidate, *American University, Washington College of Law*, 2014; B.A. American Studies, *Cornell University*, 2009. Thank you Jodie Bensman, Art Howson, and Arjun Prasad for your patience and guidance throughout this process—this work is as much a product of your dedication to the Journal as it is mine. Additionally, I give many thanks to AUBLR's editorial staff for their input. I would like to thank my parents (Clement and Geraldina), sisters (Kim, Kervina, Nashla, & Briana), and fraternal brothers from Cornell for their unconditional love and support. This work is dedicated to my nephews Gavyn, Grant, and Isaiah—I hope it serves as an example of what you three can accomplish with a little hard work and faith.

discouraging legitimate interactions with the government that may prove conducive to efficient capital markets.

TABLE OF CONTENTS

INTRODUCTION

On June 6, 2012, Washington insiders convened for breakfast at Charlie Palmer Steak Restaurant, only a few blocks from the Capitol Building.[1] The morning's discussion, titled "Defining Political Intelligence,"[2] examined the future of an opaque industry.[3] At the event, panelists defined political intelligence as the "process for collecting industry policy research" and "the deliverables of collected information (reports and analysis) sold to

1. *See Political Intelligence Panel Discussion Concludes With Recognized Need for Increased Disclosure of Non-Public Material Collection and Use*, BUS. WIRE (June 12, 2012, 8:00 AM), http://www.businesswire.com/news/home/20120612005322/en/Political-Intelligence-Panel-Discussion-Concludes-Recognized-Increased [hereinafter *Political Intelligence Panel*] (summarizing the details of a panel discussion organized by Washington lobbyists, attorneys, and policy analysts interested in the political intelligence industry).

2. *Id.*

3. *See generally* Press Release, Sen. Chuck Grassley, Grassley Seeks Same Transparency from Political Intelligence Professionals as Lobbyists (Feb. 2, 2012), *available at* http://www.grassley.senate.gov/news/Article.cfm?customel_dataPageID_1502=38833 (discussing the need for transparency around an obscure industry).

customers."[4]

The panel convened approximately two months after President Barack Obama signed into public law the Stop Trading on Congressional Knowledge Act ("STOCK Act").[5] The STOCK Act reinforces the duty of trust and confidence owed by congressional members and staffers to Congress and the American people[6] and declares a similar duty within the other branches of government.[7] The law explicitly subjects individuals employed by the government to liability for trading securities on the basis of material, nonpublic information obtained through their positions.[8]

Regarding the political intelligence industry, Section 7 of the STOCK Act merely instructs the Comptroller General of the United States to release a report on the role political intelligence plays in the financial markets.[9] Despite the STOCK Act's silence on selling policy analysis based on political intelligence (some of which may be considered "material" and "nonpublic"), Washington attorneys have speculated that the STOCK Act, in conjunction with traditional insider trading principles, may already expose political intelligence professionals to liability.[10]

---

4. *Political Intelligence Panel*, *supra* note 1.

5. *See* Press Release, White House, FACT SHEET: The STOCK Act: Bans Members of Congress from Insider Trading (Apr. 4, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/04/04/fact-sheet-stock-act-bans-members-congress-insider-trading (announcing the enactment of the STOCK Act and detailing its provisions).

6. *See* Stop Trading on Congressional Knowledge Act of 2012 (STOCK Act), Pub. L. No. 112-105, 126 Stat. 291 (2012).

7. *See id.* § 9 (incorporating employees and officers within the Executive and Judicial branches under the purview of the STOCK Act by simply compelling the Judicial Conference of the United States and the Office of Government Ethics to provide interpretive guidance on standing ethics statutes and regulations).

8. *See generally* JACK MASKELL, CONG. RESEARCH SERV., R 42495, THE STOCK ACT, INSIDER TRADING, AND PUBLIC FINANCIAL REPORTING BY FEDERAL OFFICIALS (2012) (breaking the STOCK Act into four major features, including its clarification of a public official's duty of trust and confidence to the American people, a provision that opens public officials to insider trading liability).

9. STOCK Act § 7. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-389, POLITICAL INTELLIGENCE: FINANCIAL MARKET VALUE OF GOVERNMENT INFORMATION HINGES ON MATERIALITY AND TIMING (2013) (considering the extent to which investors rely on political information, whether such practices implicate established securities laws, yet providing no recommendations for legislatures beyond balancing the costs and benefits of a disclosure regime).

10. *See* ARNOLD & PORTER LLP, ADVISORY: STOCK ACT EXPANDS INSIDER TRADING LIABILITY: COMMUNICATING WITH GOVERNMENT OFFICIALS CARRIES NEW RISKS 1–4 (2012), http://www.arnoldporter.com/resources/documents/Advisory%20STOCK_Act_Expands_Insider_Trading_Liability_Communicating_with_Government_Officials_Carries_New_Risks.pdf (advising clients to be more cautious when using information obtained from federal employees and officials); DAVIS POLK & WARDWELL LLP, CLIENT MEMORANDUM: THE STOCK ACT: IMPLICATIONS FOR TRADING ON POLITICAL INTELLIGENCE 1 (2012), http://www.davispolk.com/files/Publication/4af2e74c-700d-4f4e-970f-

This Note examines the impracticality of applying traditional insider trading principles to political intelligence activity. Furthermore, it considers an alternative interpretation of our securities laws' purview over the political intelligence industry, based on common law understandings of fraud, while acknowledging the realities of information sharing in Washington. Finally, it concludes that interpreting the STOCK Act based on fundamental principles of fraud would provide practical standards for political intelligence professionals, many of whom engage in legitimate policy research and analysis that is conducive to efficient capital markets.

I. FROM THE STOCK MARKET'S CRASH TO THE STOCK ACT: AN EVOLUTION OF SECURITIES LAWS

The Securities Exchange Act of 1934 ("SEA") was a political byproduct of the stock market's failure during the Great Depression.[11] Concerned with "ineptitude and/or chicanery" among stockbrokers and investment bankers, policymakers passed sweeping legislation to restore confidence within the market.[12]

Pursuant to the SEA,[13] the Securities and Exchange Commission ("SEC") promulgated Rule 10b-5, which prohibits individuals from engaging in deceptive practices in connection with the purchase or sale of any security.[14] Although the term "insider trading" is not statutorily defined, the SEC and courts construe Rule 10b-5 to prohibit "insider trading"—a phenomenon not limited to corporate insiders, which is something the term may suggest.[15] Generally, insider trading includes all

---

8c3f00d63e6c/Presentation/PublicationAttachment/6edb24cd-f22d-4c36-a4bb-8d0e9e3f5373/033012_STOCK_Act.pdf (advising market participants who engage public officials to access relationships with such officials before trading in order "to ensure that there is not a relationship of trust and confidence that could give rise to insider trading liability based on a misappropriation theory"); Robert L. Walker, *The STOCK Act: Insider Trading on Government Information; Corporate and Individual Compliance Concerns*, WILEY REIN LLP (Apr. 4, 2012), http://www.wileyrein.com/publications.cfm?sp=articles&id=7953 (suggesting training on the likely pitfalls the STOCK Act could pose to professionals who obtain market sensitive information from federal employees).

11. *See* George J. Benston, *Required Disclosure and the Stock Market: An Evaluation of the Securities Exchange Act of 1934*, *in* 2 THE SELECTED WORKS OF GEORGE J. BENSTON 66, 66 (James Rosenfeld ed., 2010) (describing how the Depression-era Congress wanted federal approval of all securities sales and how President Roosevelt preferred disclosure by corporations who sold their securities).

12. *See id.* (highlighting the stock market crash of 1929 and the subsequent Great Depression as the basis for the subsequent financial reform laws).

13. Securities Exchange Act § 901, 15 U.S.C. § 78a (2006).

14. 17 C.F.R. § 240.10b-5 (2012).

15. *See* Robert J. Kuker, Comment, *Insider Trading Liability of Tippees and Quasi-Insiders: Crime Shouldn't Pay*, 22 J. MARSHALL L. REV. 295, 295 n.1 (1988) (analyzing the nonobvious legal interpretation of the phrase "insider trading").

unlawful trading based on material, nonpublic information, regardless of whether the trader is a corporate insider.[16]

Notwithstanding the broad applicability of the SEA, the STOCK Act represented an expansion beyond our securities laws' original foundation in fiduciary duty principles.[17] Consequently, legal scholars and practitioners have sought ways to best fit political intelligence activity within our established securities law regime. It has been argued that political intelligence activity is most susceptible to insider trading liability under the misappropriation theory as it applies to "tippers" (those who divulge nonpublic, material information) and "tippees" (those who receive nonpublic, material information).[18] The misappropriation theory, described in *United States v. O'Hagan*,[19] considers trading on material, nonpublic information unlawful when one owes a duty of trust and confidence to the source of the information, but not necessarily to the company as a whole. Courts have held tippers and tippees liable for trading on misappropriated information when certain requirements are met.[20] Under the tipper/tippee model, liability is imposed on a tippee when the tipper has breached a fiduciary duty by divulging material, nonpublic information, and the tippee knows or has reason to know that the breach has occurred.[21] When it is difficult to determine the extent to which information is material or nonpublic, however, the otherwise straightforward tippee/tipper liability rule may be difficult to apply, a difficulty that arises when applying this rule to the emerging political intelligence industry.

---

16. *See id.*

17. *See Preventing Unfair Trading by Government Officials: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Servs.*, 111th Cong. 49 (2009) [hereinafter *Preventing Unfair Trading by Government Officials*] (statement of J.W. Verret, Assistant Professor, George Mason Univ. Sch. of Law) (providing concerns about the STOCK Act's potential unintended consequences since it expands insider trading beyond the theory's foundational principles).

18. *See The Stop Trading on Congressional Knowledge Act: Hearing Before the H. Comm. on Fin. Servs.*, 112th Cong. 81 (2011) (statement of Robert Khuzami, Director of the Div. of Enforcement, U.S. Sec. & Exch. Comm'n) (analyzing the applicability of insider trading laws to congressional members, staffers, and others who may receive and trade on material, nonpublic political intelligence).

19. 521 U.S. 642, 652 (1997) (defining the misappropriation theory of insider trading).

20. David T. Cohen, Note, *Old Rule, New Theory: Revising the Personal Benefit Requirement for Tipper/Tippee Liability Under the Misappropriation Theory of Insider Trading*, 47 B.C. L. REV. 547, 561–62 (2006) (noting that tipper/tippee liability applies in the context of the misappropriation theory, although courts are divided on whether a personal benefit is a necessary element similar to tipper/tippee liability under the classical theory).

21. *See id.* (providing the uncontested elements of tipper/tippee liability as it applies under the misappropriation theory, yet acknowledging elements of the theory that are still contested in the courts).

II. THE MOST VEXING ISSUES POSED BY THE STOCK ACT AND THE IMPRACTICALITY OF APPLYING TRADITIONAL INSIDER TRADING PRINCIPLES

Congressional silence on the STOCK Act's purview over the political intelligence industry and no indication of guidance from the SEC led practitioners to speculate on the STOCK Act's reach.[22] Some of the most vexing issues for practitioners include applying the (1) material and (2) nonpublic elements of the misappropriation theory to political intelligence activity.[23] This Section will examine the application of these elements in turn.

A. The Material Element

Depending on the facts, courts approach the materiality element of insider trading in two different ways. Normally, courts consider whether it is likely that the inside information "would have assumed actual significance in the deliberations of a reasonable investor."[24] Contrarily, when dealing with speculative and/or contingent material information, courts apply a probability/magnitude test that considers the likelihood of an anticipated event and its potential financial impact.[25] Scholars anticipate that the probability/magnitude test is most applicable to political intelligence activity given the speculative nature of the legislative process.[26]

---

22. *See* ARNOLD & PORTER LLP, *supra* note 10, at 1–2, 4 (speculating that the STOCK Act's language may already impose liability on political intelligence professionals); DAVIS POLK & WARDWELL LLP, *supra* note 10, at 2–3 (cautioning that due to the STOCK Act's language in conjunction with the misappropriation theory, one should consider the nature of the information obtained on Capitol Hill before selling that information, or trading upon it). *See generally* Walker, *supra* note 10.

23. *See* Kenneth A. Gross, *Unique Issues Facing Companies Under the STOCK Act*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (May 3, 2012, 9:24 AM), http://blogs.law.harvard.edu/corpgov/2012/05/03/unique-issues-facing-companies-under-the-stock-act/ (discussing the difficulties of applying insider trading principles under the STOCK Act to political intelligence activities given a public official's unique access to information and the official's duty to interact with constituents).

24. *See* Bradley J. Bondi & Steven D. Lofchie, *The Law of Insider Trading: Legal Theories, Common Defenses, and Best Practices for Ensuring Compliance*, 8 N.Y.U. J. L. & BUS. 151, 179 (2011) (considering that the materiality element of the misappropriation theory is a high standard established by courts in order to protect shareholders from useless information that is not conducive to informed decision-making).

25. *See id.* at 180 (examining an alternative approach to determining the materiality of market-sensitive information when material, nonpublic information pertains to speculative matters similar to mergers, acquisitions, and bankruptcies).

26. *See Preventing Unfair Trading by Government Officials*, *supra* note 17, at 33–35 (statement of Peter J. Henning, Professor of Law, Wayne State Univ. Law Sch.) (hinting at the notion that the legislative process's unpredictable nature would best fit the probability/magnitude materiality test).

Applying the probability/magnitude test to legislative action in a meaningful way, however, is problematic given the general uncertainty that introduced legislation would eventually be enacted by Congress.[27] Take the 111th Congress' legislative record. Between 2009 and 2010, members of Congress introduced 10,629 bills for consideration.[28] Only ten percent of those bills underwent some form of legislative activity beyond simply being referred to a committee.[29] Furthermore, only 366 laws were passed in the 111th Congress, a mere thirty-six percent of bills that underwent legislative activity beyond the committee level; ultimately, only three percent of bills introduced in the 111th Congress became public law.[30]

These statistics may reflect the numerous obstacles within the legislative process, including necessary voting on the committee level and on each chamber's floor,[31] reconciliatory proceedings between both chambers,[32] and a necessary signature or veto from the President.[33] Furthermore, a host of non-legislative factors may impact the legislative process,[34] making it difficult to consider truly any one piece of political intelligence material on its own.[35] These realities of the legislative process would likely trigger the "mosaic defense" against insider trading allegations,[36] a shield based on the legal rule that "an investor [who] assembles multiple pieces of non-material information to reach a material conclusion has not violated insider trading

27. *See* Josh Tauberer, *Kill Bill: How Many Bills Are There? How Many Are Enacted?*, GOVTRACK.US (Aug. 4, 2011), http://www.govtrack.us/blog/2011/08/04/kill-bill-how-many-bills-are-there-how-many-are-enacted/ (noting that the 111th Congress enacted only three percent of legislation introduced).

28. *Id.*

29. *Id.*

30. *Id.*

31. *See* JOHN V. SULLIVAN, HOW OUR LAWS ARE MADE, H.R. Doc. No. 110-49, at 37 (2007) (stating that after the House of Representatives has considered a bill the "Senate committees give the bill the same detailed consideration as it received in the House and may report it with or without amendment").

32. *See id.* at 41–48 (detailing the conference process to reconcile conflicting bills between the Senate and the House).

33. *See generally id.* at 50–51 (detailing the veto process within the larger legislative process).

34. Benjamin I. Page & Robert Y. Shapiro, *Effects of Public Opinion on Policy*, 77 AM. POL. SCI. REV. 175, 186 (1983) (arguing that public opinion influences policy, while acknowledging that there may very well be other influences, including world events, interest group campaigns, and other exogenous factors).

35. *See E-Alert: STOCK ACT Spotlights Trading on Government Information*, COVINGTON & BURLING LLP 1, 5 (2012), http://www.cov.com/files/Publication/7f2980b7-4773-4b5b-b7bc-3b2e10aedb1a/Presentation/PublicationAttachment/fcfc6963-f48f-4320-a19e-416fba589ac3/STOCK_Act_Spotlights_Trading_on_Government_Information.pdf (noting that groups that engage Members of Congress and their staff would likely acknowledge that information they obtained is not material individually, although such an argument would not prevent prosecutorial action by the SEC).

36. *See id.*

laws, regardless of whether the information obtained was nonpublic."[37] Considering the varying factors that affect the legislative process, and the rarity that any political intelligence would be considered material individually, applying the probability/magnitude standard to a piece of political information may be an issue that would take years to resolve.[38]

B. The Nonpublic Element

Information is considered public when it has been dispersed widely among investors with no special regard to any particular person or class.[39] Even after such information has been disclosed, it is considered nonpublic until it has been communicated so widely that stock prices reflect the availability of such information.[40] Furthermore, factors considered when determining if information is nonpublic includes the following: (1) whether the information is public through the Dow Jones business information service; (2) whether the information has been disseminated through "wire services, such as AP or Reuters, radio, television, or the Internet"; (3) whether the information has been circulated through a general news service (such as *The Wall Street Journal* or *Business Week*); and (4) whether the information has been disclosed through public documents filed with the SEC.[41]

Given the unique nature of information sharing that is encouraged within the halls of Congress, the applicability of the nonpublic element will remain a cumbersome legal issue for a number of reasons.[42] Congressional committee meetings and hearings are an example of how Capitol Hill's unique nature complicates the applicability of insider trading laws. Clause 2(g)(1) of Rule XI of the Rules of House of Representatives provides that "[e]ach meeting for the transaction of business, including the mark up of legislation, by a standing committee or subcommittee thereof (other than the Committee on Ethics or its subcommittees) shall be open to the public,

37. Bondi & Lofchie, *supra* note 24, at 154 (emphasis removed).

38. *See* COVINGTON & BURLING LLP, *supra* note 35, at 6.

39. *See* SEC v. Suman, 684 F. Supp. 2d 378, 388 (S.D.N.Y 2010) (synthesizing case law in order to determine when information should be considered material, nonpublic information).

40. *See* United States v. Royer, 549 F.3d 886, 898 (2d Cir. 2008) (affirming a district court's jury instruction that information is considered public after stock prices have "an opportunity to 'absorb' the disclosed information . . .").

41. *See* CORPORATE COUNSEL GUIDE TO INSIDER TRADING & REPRESENTATION § 18:4 (2012 ed.) (noting that tangible evidence that information has been disseminated to investors serves as the best indicator of whether information should be considered public).

42. Gross, *supra* note 23 (analyzing the difficulties of determining when congressional information should be considered "public" or "nonpublic" given the nature of communication on Capitol Hill).

including to radio, television, and still photography coverage."[43] With a few exceptions, mostly all official congressional committee meetings are public, and many can be viewed live on television or the Internet.[44]

Although most congressional proceedings are accessible to the public, it is unclear to what extent information obtained from such meetings is considered "public" under our insider trading laws.[45] Consider the following real-life scenario. During the mid-2000's, Congress considered legislative remedies for Americans who suffered from asbestos-related injuries, which included establishing a $140 billion government-backed trust fund for claims against manufacturers who used asbestos.[46] During those proceedings, hedge funds employed "line sitters" and other political intelligence operatives to hold seats at committee hearings.[47] Given the legislation's potential impact on the stock prices of companies with asbestos-illness liability, political intelligence operatives were able to profit from the information they obtained.[48]

Notwithstanding the theoretic public nature of congressional hearings, attendees fortunate to reserve a space are privy to potentially market-sensitive information before the larger American public. Therefore, in practice, the larger American public would have to wait to obtain such information through television access (if aired), news articles (if covered), or word of mouth (if fortunate). Such information has the potential of becoming worthless by the time it is well-known because of the ever-changing nature of the market.[49] Investors and political intelligence operatives are left to wonder exactly when congressional information is "public."[50] Such a lack of clarity would leave market researchers with

43. KAREN L. HAAS, CLERK, H.R., 112TH CONG., RULES ON THE HOUSE OF REPRESENTATIVES, R. XI, at 17–18 (2011).

44. *See id.* (providing official protocol that encourages public access to congressional meetings and hearings).

45. *Cf.* Gross, *supra* note 23 (pointing out that while televised congressional proceedings would certainly be considered "public," an insider trading analysis of political intelligence would be more difficult where proceedings are open to a smaller number of persons, are not televised, or are conducted in private).

46. *See* Bud W. Jerke, Comment, *Cashing in on Capitol Hill: Insider Trading and the Use of Political Intelligence for Profit*, 158 U. PA. L. REV. 1451, 1453–54 (2010) (noting the relevancy of mesothelioma cases to the political intelligence industry and market participants).

47. *See Political Intelligence Panel*, *supra* note 1.

48. *See* Jerke, *supra* note 46, at 1453 (indicating that after asbestos legislation narrowly passed the Senate Judiciary Committee in 2003, shares of USG Corporation, a construction materials manufacturer, rose by 8.3% because the company had asbestos-related tort liabilities).

49. *See* Sisira Kanti Mishra, *Capital Market Efficiency* 1 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1942820 (describing the nature of efficient capital markets that adjust to new information).

50. *See* ARNOLD & PORTER LLP, *supra* note 10, at 3 (speculating about the STOCK

fewer incentives to seek out political intelligence.[51]

III. CONSIDERING AN ALTERNATIVE APPROACH TO POLITICAL INTELLIGENCE ACTIVITY BASED ON COMMON LAW PRINCIPLES OF FRAUD

In his dissent in *Chiarella v. United States*, Chief Justice Burger offered an alternative approach to insider trading that holds liable those who benefit from information "unlawfully converted for personal gain."[52] According to Chief Justice Burger, whether trading on material, nonpublic information is illegal should turn on whether an investor exploits an "ill-gotten informational advantage."[53] Consequently, this reading of Rule 10b-5 allows a safe harbor for professionals who benefit from material information that is not generally known, but was still acquired lawfully.[54]

Burger's reasoning in *Chiarella* has its roots in common law principles.[55] Under the common law, whether a party has a duty to disclose information during a business transaction should be determined, in part, by considering: (1) whether the information is extrinsic or intrinsic to the transaction; (2) whether there is an unusual difference in intelligence among transacting parties; and (3) whether material, nonpublic information was obtained illegally instead of through legitimate diligence.[56]

An early example of how these principles may apply to political intelligence activity can be found in the landmark Supreme Court case *Laidlaw v. Organ*.[57] In *Laidlaw*, two parties contracted for the sale of tobacco.[58] The buyer possessed what amounted to valuable political

---

Act's potential scope).

51. *See* Jerke, *supra* note 46, at 1518 (addressing the potential chilling effect on congressional engagement if insider trading is expanded to regulate political intelligence activities).

52. *See* Chiarella v. United States, 445 U.S. 222, 243 (1980) (5–4 decision) (Burger, C.J., dissenting) (providing an alternative interpretation of insider trading precedent and statutory language to provide legal room for market specialists to perform their everyday functions).

53. *See id.* at 245.

54. *See id.* at 242–43 ("[M]arket specialist would not be subject to a disclose-or-refrain requirement in the performance of their everyday market functions. [In this instance], trading is accomplished on the basis of material, nonpublic information, but the information has not been unlawfully converted for personal gain.").

55. *See* Donald C. Langevoort, *Words From On High About Rule 10b-5:* Chiarella*'s History*, Central Bank*'s Future*, 20 DEL. J. CORP. L. 865, 883 (1995) (explaining how the reasoning in Burger's dissent in *Chiarella* has its roots in principles established through common law).

56. *See* W. Page Keeton, *Fraud—Concealment and Non-Disclosure*, 15 TEX. L. REV. 1, 34–35 (1936) (providing a number of factors that should be considered when determining whether nondisclosure amounts to fraud).

57. 15 U.S. (2 Wheat.) 178 (1817).

58. *See id.*

intelligence—information that indicated the War of 1812 had ended by way of a treaty between the United States and England.[59] Consequently, an embargo was lifted, substantially raising the price of tobacco.[60] The Court held that a party in a similar situation does not have a duty to disclose when the information at question pertains to extrinsic circumstances, is equally accessible, and has been obtained lawfully.[61]

The remainder of this Section will examine how these principles may be applied to contemporary scenarios that are common in Washington.

A. Is the Political Intelligence Extrinsic or Intrinsic?

Under common law, whether information is material depends on the extent to which the information is considered intrinsic.[62] Intrinsic information pertains to "the very ingredients" of a transaction; contrarily, extrinsic information forms "no part of" the transaction, notwithstanding the possibility that such information may very well induce a party into a transaction.[63]

For an illustration of how this principle may apply to political intelligence, compare the Emergency Economic Stabilization Act with Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"). Both pieces of legislation pertained to the financial markets.[64] While the Emergency Economic Stabilization Act authorized the Department of Treasury to purchase $700 billion in failed assets,[65] including mortgage-backed securities,[66] Title X of Dodd-Frank established the Bureau of Consumer Financial Protection, which has broader authority.[67] Possessing inside knowledge from the Hill or from the

59. *See id.* at 183.

60. *See id.* (noting the price of tobacco increased thirty to fifty percent).

61. *See id.* at 194.

62. *See* Keeton, *supra* note 56, at 20 (discussing fundamental common law principles of fraud, including the general idea that intrinsic facts, more so than extrinsic facts, should be disclosed during a transaction).

63. *See id.* (distinguishing circumstances that are extrinsic to a transaction from those that are intrinsic).

64. *Compare* Emergency Economic Stabilization Act of 2008 § 115, 12 U.S.C. §§ 5201–02 (Supp. IV 2011) (seeking "to restore liquidity and stability to the financial system of the United States . . . ."), *with* Dodd-Frank Act § 1011, 12 U.S.C. § 5491 (Supp. IV 2010) (creating an independent agency with oversight of consumer financial products and services).

65. 12 U.S.C. § 5225.

66. *See* BAIRD WEBEL, CONG. RESEARCH SERV., R41427, TROUBLED ASSET RELIEF PROGRAM (TARP): IMPLEMENTATION AND STATUS 2–3 (2012) (describing the Public-Private Investment Program of the 2008 bailout program and its status at relieving banks from failed mortgage-backed securities).

67. *See* DAVID H. CARPENTER, CONG. RESEARCH SERV., R42572, THE CONSUMER FINANCIAL PROTECTION BUREAU 1 (2012) (explaining that the newly established Bureau of Consumer Financial Protection has rulemaking power over "many consumer

Treasury Department regarding which banks would be injected with bailout money would certainly amount to intrinsic information under common law.[68] However, Title X's oversight of mortgage servicing pertained to countless financial institutions, making inside knowledge of its broad provisions extrinsic to the markets they affected.[69]

B. Is There an Unusual Advantage?

The common law also disfavors unusual advantages in information.[70] Consider private meetings where official legislative and executive business is conducted. In the midst of the 2008 financial crisis, President George W. Bush and congressional leaders negotiated on how $700 billion in federal aid to the financial markets would be distributed.[71] The meeting's attendees included the House Speaker, the Senate Majority Leader, chairmen of powerful committees, and the two presidential hopefuls, future President Barack Obama and Arizona Senator John McCain.[72] The meeting was mostly a closed session, opening only for photographic documentary and brief remarks from the President.[73] In the event that an insider with permission to attend became aware of the negotiated agreements on the allocation of bailout funds, that insider would have an unusual advantage in information.[74] Under the common law, the hypothetical insider may trigger a duty to disclose due to his unusual access into closed White House proceedings.[75]

---

financial products and services, as well as the entities that sell them").

68. *Cf.* Keeton, *supra* note 56, at 20 (providing insight on what information should be disclosed depending on the information's intrinsic nature).

69. *Cf. id.* (defining extrinsic information as facts that are "accidentally connected with" the essence of a transaction, rather than "bear[ing] upon it," even though that information may very well affect pricing during a transaction).

70. *See id.* at 34.

71. *See* Elisabeth Bumiller & Jeff Zeleny, *With Debate Uncertain, Candidates Meet with Bush*, N.Y. TIMES (Sept. 25, 2008), http://www.nytimes.com/2008/09/26/us/politics/26debatecnd.html?pagewanted=all&_r=0 (summarizing the proceedings during the 2008 bailout meeting at the White House, a negotiation session that led to no consensus).

72. *See* Mark Silva & Naftali Bendavid, *The bailout parley: How it went down; Tracing McCain and Obama's capital steps*, CHI. TRIB. (Sept. 26, 2008), http://articles.chicagotribune.com/2008-09-26/news/0809251043_1_john-mccain-obama-campaign-john-boehner (describing the closed-door bailout meeting which lasted for approximately fifty-seven minutes, ending with a lawmaker simply stating, "[a]ll I can say is, we had an interesting meeting with the president and vice president, Sen. Obama and Sen. McCain").

73. *Id.*

74. *Cf.* Keeton, *supra* note 56, at 34 (explaining why using unusual advantages in information suggests that a party has a greater duty to disclose his extraordinary knowledge prior to a business transaction "simply because our sense of justice demands it" to avoid fraud).

75. *Cf. id.* (acknowledging that where information is equally accessible, and where

C. *Was the Information Obtained Through an Affirmative Deceitful Act, or Is It a Product of Diligence?*

Common law disfavors investors who benefit from information obtained illegally or deceptively.[76] Consider congressional meetings, hearings, and markups that are closed to the public.[77] Some meetings regarding national defense are conducted in private, and such legislative activity may also have an impact on certain markets.[78] If an investor intentionally misrepresented herself as a congressional staff member to gain access to a defense budget hearing, under the common law, that information should be disclosed prior to a business transaction due to its illegal and deceptive acquisition.[79]

Furthermore, under common law, an investor would be compelled to prevent another's reliance on misrepresented material information that investor learns to be false.[80] Take the Supreme Court's recent ruling on the Affordable Care Act ("ACA"). After the ruling was released and confirmed, stock prices in hospital companies increased, while those in insurance companies fell immediately.[81] While the ruling was being announced, however, there were conflicting reports by news media on how the Court ruled on the ACA's individual mandate.[82] Although there were reports stating that the Court overturned the individual mandate, those

---

diligent effort would make it attainable to anyone, an unfair advantage does not exist, regardless of the number of people with such knowledge).

76. *See id.* at 35 (explaining that the manner in which information is acquired may determine whether disclosure is legally required).

77. *See* HAAS, *supra* note 43.

78. *See, e.g.*, Jeremy Herb, *Defense Contractors Hesitate Over Issuing Layoff Notices Before Election*, THE HILL (Sept. 9, 2012, 5:00 AM), http://thehill.com/blogs/defcon-hill/industry/248313-defense-contractors-hesitate-over-layoff-notices-before-election (noting that major defense contractors have threatened layoffs in fear of automatic budget cuts looming at the end of the 112th Congress if a budget deal is not met).

79. *Cf.* Keeton, *supra* note 56, at 35 (suggesting that information that affects the value of the subject-matter of a transaction should be disclosed when obtained by an illegal act).

80. *Cf. id.* at 6 (elaborating on how the common law disfavors a party continuing misrepresentations when they are aware of the falsehood and have an opportunity to prevent reliance thereon).

81. *See Supreme Court's Health Care Ruling Touches Stock Market, Political Campaigns*, ASSOCIATED PRESS, June 28, 2012, *available at* http://www.pennlive.com/midstate/index.ssf/2012/06/supreme_courts_health_care_rul_1.html (discussing the financial impact of the Supreme Court's 2012 health care ruling).

82. *See* Brian Stelter, *CNN and Fox Trip Up in Rush to Get the News on the Air*, N.Y. TIMES (June 28, 2012), http://www.nytimes.com/2012/06/29/us/cnn-and-foxs-supreme-court-mistake.html (describing how some media outlets incorrectly reported the Supreme Court's 2012 health care ruling).

reports were false.[83] Consistent with common law principles of fraud, once media officials realized they reported inaccurate information on the ACA's ruling, they assumed a duty to disclose accurate information or abstain from trading, if they were involved in trading impacted by the ruling.[84] Such active concealment during a business transaction is fraudulent as a matter of law.[85]

IV. MOVING FORWARD: HOW THE STOCK ACT CAN BE MADE MORE FUNCTIONAL BY APPLYING COMMON LAW PRINCIPLES TO POLITICAL INTELLIGENCE ACTIVITY

While the STOCK Act directs Congress's ethics committees, the U.S. Office of Government Ethics, and the Judicial Conference of the United States to provide interpretive guidance to individuals working within the three branches of government,[86] the Act has little to say about outsiders who engage government officers and employees daily.[87] Accordingly, political intelligence professionals have been left to speculate on how their profession fits under the STOCK Act's authority.[88]

Moving forward, Congress, the SEC, or both should take action. While Congress should clarify its intent in enacting the STOCK Act, the SEC should provide interpretive guidance on how its securities laws apply to political intelligence activity. Either way, both Congress and the SEC should consider fundamental principles of fraud established under common law and alluded to in Chief Justice Burger's *Chiarella* dissent.[89] While political intelligence obtained through affirmative misrepresentations or illegal acts should have no place in the financial markets, political intelligence acquired through "exceptional knowledge, skill, or effort" should be permissible.[90] Such permission would incentivize the exploration of political information, which may in turn encourage a more efficient market place.[91]

---

83. *See id.* (detailing the confusion surrounding the Supreme Court's decision on the health care ruling).

84. *Cf.* Keeton, *supra* note 56, at 36 (considering the question of whether an affirmative action prevented a party from discovering information as a factor used to determine fraud).

85. *Cf. id.* at 37 ("The active concealment of anything that might prevent the purchaser from buying at the price agreed on, is, and should be, as a matter of law fraudulent.").

86. STOCK Act §§ 3, 9.

87. *See id.*

88. *See generally* ARNOLD & PORTER LLP, *supra* note 10, at 4–5.

89. *See* Chiarella v. United States, 445 U.S. 222, 243–44 (1980); Langevoort, *supra* note 55, at 883.

90. *See* Keeton, *supra* note 56, at 26.

91. *See* Jerke, *supra* note 46, at 1520 ("Mining nonpublic information does not simply help the direct recipient of the information, but encourages accuracy of prices,

CONCLUSION

Professor W. Page Keeton once noted that "a decision on a particular state of facts may be desirable today, whereas the same decision a hundred years from now might be undesirable as not sub-serving the best interests of society."[92] The legal community is in a similar situation today as it attempts to apply traditional insider trading principles to a relatively new phenomenon—the commodification of political intelligence. Accordingly, Congress and the SEC should approach the political intelligence industry cautiously, considering the practicality of applying traditional insider principles to a profession that furthers favorable market research. As this Note suggests, there may be value in considering fundamental principles of fraud established under common law, hinted to by Chief Justice Burger in his *Chiarella* dissent. Nonetheless, this very debate may be an indicator that lawmakers should consider overhauling our insider-trading regime altogether. Indeed, the expansion of traditional insider trading principles to cover political activity signals a clear policy shift from 1934 to the present. Comprehensive reform and a clear indication of legislative intent may be needed to avoid the risk of uncertainty among participants within our capital markets.

efficiency of markets, and protection of all investors.").

92. *Cf.* Keeton, *supra* note 56, at 34.

* * *

AMERICAN UNIVERSITY BUSINESS LAW REVIEW

SUBSCRIPTION ORDER FORM

Subscription Options (check one):

_____ $30.00 Alumni Subscription

_____ $45.00 Domestic Subscription

_____ $50.00 Foreign Subscription

_____ $20.00 Single-Issue Only

_____ **Please check here if you would like to enclose a check for the amount selected.**

Please complete the form below and send it with your check made payable to *American University Business Law Review* at:

American University Business Law Review
Washington College of Law
4801 Massachusetts Ave., N.W.
Suite 615A
Washington, D.C. 20016
Attn: Journal Coordinator

_____ **Please check here if you would like to receive an invoice for the amount selected.**

Please complete the form below and email it to Sharon Wolfe, the Journal Coordinator, at shuie@wcl.american.edu.

Please begin my subscription with Volume _____ Single-Issue only _____

Name:

_____

Institution:

_____

Address:

_____

City, State, Zip:

_____

*Subscriptions are automatically renewed unless cancellation is requested.

* * *

* * *

* * *