ECONOMIC ESPIONAGE AS REALITY OR RHETORIC: EQUATING TRADE SECRECY WITH NATIONAL SECURITY

by
Rochelle Cooper Dreyfuss[*] *and Orly Lobel*[**]

In the last few years, the Economic Espionage Act (EEA), a 1996 statute that criminalizes trade secret misappropriation, was amended twice, once to increase the penalties and once to expand the definition of trade secrets and the types of behaviors that are illegal. Recent developments also reveal a pattern of expansion in investigation, indictments, and convictions under the EEA as well as the devotion of large resources by the FBI and other agencies to warn private industry against the global threats of trade secret theft. At the international level, the United States government has been advocating enhanced levels of trade secret protection in new regional trade agreements. This Article asks about the effects these developments on innovation. The Article examines the rhetoric the government is using to promote its trade secret agenda, uncovering that the argument for greater protection appears to derive at least some of its power from xenophobia, and most importantly, from a conflation of private economic interests with national security concerns, interjecting a new dimension to the moral component of innovation policy debates. Analyzing recent empirical research about innovation policy, we ask about the effects of these recent trends on university research and on private market innovation, including entrepreneurship, information flows, and job mobility. We argue that, paradoxically, the effort to protect valuable information and retain the United States' leadership position could disrupt information flows, interfere with collaborative efforts, and ultimately undermine the inventive capacity of American innovators. The Article offers suggestions for reconciling legitimate concerns about national security with the balance intellectual property law traditionally seeks to strike between incentivizing innovation and ensuring the vibrancy of the creative environment. We conclude that a legal regime aimed at protecting incumbency is not one that can also optimally foster innovation.

[*] Pauline Newman Professor of Law, New York University School of Law.

[**] Don Weckstein Professor of Labor and Employment Law, University of San Diego School of Law.

The film begins with footage of an apartment building in flames. Chinese music plays in the background. The voice-over, in Chinese, transmits urgency.

Soon an impecunious American engineer is approached by a Chinese company keen to produce better insulation. At first intrigued by a generous financial offer, the engineer eventually decides the Chinese are trying to discover his firm's secret technology. He informs his employer; the firm tells the FBI. An investigation ensues: the wrongdoers are caught, tried, and convicted of economic espionage. A hero, the engineer (although still strapped for cash) has saved his firm, the jobs of all its employees, and the one-company town in which it is situated.

The film concludes with another voice-over, this one in English: "[T]heft of trade secrets robs up to $400 billion a year from the U.S. economy."

–The Company Man: Protecting America's Secrets (2012)

INTRODUCTION

The strong production values suggest MGM, United Artists, perhaps an indie or made-for-TV movie. But it is none of the above. *The Company Man*, "a cautionary tale" for high tech firms, was produced in 2012 by the FBI Counterintelligence Section, Strategic Partnership Unit, in collaboration with Rocket Media.[1] Much like a Hollywood film, the FBI first tested it, then, in July 2015, rolled it out officially during a nationwide economic espionage awareness campaign.[2]

As the production of this film suggests, the United States has become very serious about protecting trade secrets. In the last few years, the Eco-

[1] FBI, *The Company Man: Protecting America's Secrets*, YOUTUBE (July 23, 2015), https://www.youtube.com/watch?v=Gy_6HwujAtU; *see also Dramatic Narrative*, ROCKET MEDIA (2013), http://rocket-media.wix.com/rocket-media#!dramatic-narrative/c1r1e (additional FBI short films).

[2] *Economic Espionage: FBI Launches Nationwide Awareness Campaign*, FBI (July 23, 2015), https://www.fbi.gov/news/stories/2015/july/economic-espionage/economic-espionage.

nomic Espionage Act (EEA), a 1996 statute that criminalizes trade secret misappropriation,[3] was amended twice, once to increase the penalties,[4] and then to ensure that information taken for *intended* (rather than *actual*) use is sufficient to complete the crime.[5] This change also expanded the definition of "trade secret" to include information used in "services" not merely "products" involving interstate commerce.[6] In the first five years, there were only 11 prosecutions under the Act.[7] But as the FBI channeled more resources into the investigation of trade secret cases and other government agencies improved their coordination, the number of prosecutions increased.[8] As of 2012, there were 124;[9] and in the last two years, prosecutions have increased more than 30% over the 2012 rate.[10] The government has also been busy publishing materials on economic espionage. In 2009, the Department of Justice (DOJ) devoted an entire volume of its U.S. Attorneys' Bulletin to issues arising in trade secret prosecutions;[11] in 2011, the Office of the National Counterintelligence

---

[3] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (2012).

[4] Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442 (2013) (codified as amended at 18 U.S.C. § 1831).

[5] Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (codified as amended at 18 U.S.C. § 1832(a)).

[6] *Id.* (changing "that is related to or included in a product that is produced for or placed in foreign commerce" to "that is related to a product *or service* used in or *intended for use* in interstate or foreign commerce" (emphasis added)).

[7] J. Derek Mason, Gerald J. Mossinghoff & David A. Oblon, *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, COMPUTER LAW., Mar. 1999, at 14, 18; *see also* Robin L. Kuntz, *How Not to Catch A Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 BERKELEY TECH. L.J. 901, 908–09 (2013) (describing cases prior to 2009 as "unicorn sightings").

[8] *See* Counterintelligence Enhancement Act of 2002, Pub. L. No. 107-306, §§ 901–904 116 Stat. 2383, 2432 (codified as amended at 50 U.S.C. §§ 401–402 (2012)); Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, U.S. ATTORNEYS' BULL., Nov. 2009, at 7, http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf.

[9] Peter J. Toren, *A Look at 16 Years of EEA Prosecutions*, LAW 360 (Sept. 19, 2012), http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions. According to an administration report, from 2009 to 2013, the FBI was involved in 20 cases—nearly double the total of the first five years. *See* EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS annex 3 (2013) [hereinafter STRATEGY REPORT], https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf. It is somewhat difficult to compare cases because the targets of EEA investigations can be indicted or convicted on other grounds, such as computer fraud.

[10] Nicole Perlroth, *Accused of Spying for China, Until She Wasn't*, N.Y. TIMES (May 9, 2015), http://nyti.ms/1P7ACUU.

[11] *See Economic Espionage and Trade Secrets*, U.S. ATTORNEYS' BULL. (Nov. 2009), http://www.justice.gov/sites/default/files/usao/legacy/2009/12/10/usab5705.pdf (including articles on issues arising in the prosecution of EEA cases, common

Executive (ONCIX), which acts as coordinator of government enforcement efforts, issued a report focused on the special dangers of cyber-espionage;[12] in 2012, the U.S. Defense Security Service published a major analysis of espionage aimed at U.S. technologies;[13] in 2013, the U.S. Departments of Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence, and the Office of the United States Trade Representative put out a joint plan on strategies to mitigate trade secret theft;[14] and in 2014, the Congressional Research Service published an overview report on EEA-related activities.[15] In 2015, President Obama issued an executive order to impose new sanctions on cyber-enabled activities, including bans on commercial transactions and freezing U.S. assets.[16] And Congress is now considering a civil trade secret law to back up the EEA.[17]

The United States has also upped its game at the international level. The Office of the United States Trade Representative (USTR) regularly publishes so-called Special 301 Reports examining the intellectual property practices of U.S. trading partners and places those deemed deficient on watch lists.[18] Starting in 2012, these watch lists have included strident critiques of countries that fail to "have robust systems for protecting trade secrets, including deterrent penalties for criminal trade secret theft."[19]

---

defenses, parallel proceedings, use of electronic evidence, and sentencing); *see also* COMPUT. CRIMES & INTELL. PROP. SEC., DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES (4th ed. 2013) [hereinafter IP CRIMES MANUAL].

[12] OFFICE OF THE NAT'L COUNTERINTELL. EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011 (October 2011) [hereinafter ONCIX REPORT], http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[13] DEF. SEC. SERV., TARGETING U.S. TECHNOLOGIES: A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY (2012) [hereinafter TARGETING ANALYSIS], http://www.dss.mil/documents/ci/2012-unclass-trends.pdf.

[14] STRATEGY REPORT, *supra* note 9 (acknowledging collaborative effort of administrative strategy on mitigating the theft of U.S. trade secrets).

[15] CHARLES DOYLE, CONG. RESEARCH SERV., R42681, STEALING TRADE SECRETS AND ECONOMIC ESPIONAGE: AN OVERVIEW OF 18 U.S.C. 1831 AND 1832, at 1 (2014), https://www.fas.org/sgp/crs/secrecy/R42681.pdf.

[16] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015), https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[17] *See* Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (introduced Apr. 29, 2014).

[18] *See* 19 U.S.C. § 2242(b) (2012).

[19] OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2012 SPECIAL 301 REPORT 17 (Apr. 2012), https://ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf. The report cites China in particular. *See id.* at 26–27, 31. For comparison, the 2011 Special 301 Report made no mention of trade secrets. Subsequent reports are increasingly strident. The 2014 Report specifically points out "inadequacies in trade

Specifically listed are China, India, and Thailand.[20] The Reports have met with some success—last year, the European Union (EU), which was mentioned in the 2012 Special 301 Report, promulgated a proposed directive to unify the trade secret laws of member states.[21] Nonetheless, the USTR has added enhanced levels of trade secret protection to the agenda for negotiating new regional trade agreements.[22]

Much of this activity is a dramatic break with the past. When the EEA was enacted two decades ago, the significant change it made in the institutional design of the intellectual property system was highly controversial. While federal law had long provided protection to advances that qualify for patents, copyrights, or trademarks, trade secrets were strictly the province of the states.[23] Moreover, very few violations of copyright and trademark law were regulated through the criminal law, and no

---

secret protection in China, India, and elsewhere, as well as an increasing incidence of trade secret misappropriation," OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2014 SPECIAL 301 REPORT 6 (Apr. 2014) [hereinafter 2014 REPORT], https://ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf. The report singles out China, *id.* at 31–33, India, *id.* at 42, Thailand, *id.* at 46, and the EU, *id.* at 11. The 2015 Report is similar. OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2015 SPECIAL 301 REPORT 1, 20–21 (Apr. 2015) [hereinafter 2015 REPORT], https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf. This time, the Report notes with approval the EU's proposed directive on trade secrets. *Id.* at 21. However, China is still singled out, *id.* at 32–34, 36–37, as is India, *id.* at 51. Thailand is no longer mentioned in connection with trade secrets.

[20] *See* 2014 REPORT, *supra* note 19, at 6, 16–18, 31–33 (China); *id.* at 43 (India); *id.* at 46 (Thailand).

[21] *See* 2015 REPORT, *supra* note 19, at 21; European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure*, COM(2013) 813 final (Nov. 28, 2013), http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/131128_proposal_en.pdf; s*ee also* Ping, Xiong, *China's Approach to Trade Secrets Protection: Is a Uniform Trade Secrets Law in China Needed?*, *in* THE INTERNET AND THE EMERGING IMPORTANCE OF NEW FORMS OF INTELLECTUAL PROPERTY (Susy Frankel & Daniel J. Gervais eds., forthcoming 2016).

[22] The Transpacific Partnership Agreement (TPP) was concluded in November 2015. It includes increased protection for trade secrets, including provisions for criminal penalties. *See* Trans-Pacific Partnership Agreement art. 18.78 (2), https://ustr.gov/sites/default/files/TPP-Final-Text-Intellectual-Property.pdf. Interestingly, while the Agreement requires criminalization, it gives member states substantial discretion over the elements of the crime, so long as they penalize computer hacking. It remains to be seen, however, whether the TPP will be ratified.

[23] Most states have adopted the Uniform Trade Secrets Act, UNIF. TRADE SECRETS ACT (amended 1985), 14 U.L.A. 536 (1985), but a few rely on common law and reference the RESTATEMENT OF TORTS §§ 757–758 (AM. LAW INST. 1939) or the RESTATEMENT (THIRD) OF UNFAIR COMPETITION (AM. LAW INST. 1995). In addition, several states provide criminal statutes for theft of trade secrets, for example, CAL. PENAL CODE § 499c (West 2015); N.J. STAT. ANN. § 2C:20-1 (West 2014); N.Y. PENAL LAW § 165.07 (McKinney 2015); TEX. PENAL CODE ANN. § 31.05 (West 2014).

criminal penalties attached to any form of patent infringement.[24] It was especially difficult to understand criminalization of misappropriation at the federal level because there were already several federal criminal statutes aimed at deterring truly egregious conduct, such as mail, wire, and computer fraud.[25] Indeed, a few members of Congress were so worried about the potential impact of the EEA that they insisted that, for the first five years after enactment, the Attorney General's office approve every prosecution.[26]

Similar skepticism could be observed in international law. The World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights (the WTO's TRIPS Agreement), which was promulgated around the same time as the EEA, includes only one provision on trade secrets.[27] While TRIPS requires criminal penalties for copyright piracy and trademark counterfeiting, it does not mandate criminal punishment for trade secret misappropriation.[28] To date, no completed bilateral or regional agreement includes any reference to the criminal theft of trade secrets.

The gulf between the treatment of trade secrecy and the treatment of copyright and trademark violations is not surprising, for the effects of

---

[24] The exceptions are piracy, counterfeiting, and bootlegging. *See* 18 U.S.C. § 2318 (2012) (trafficking in counterfeit labels); 18 U.S.C. § 2319 (2012) (criminal infringement of copyright); 18 U.S.C. § 2319A (2012) & 18 U.S.C. § 2319B (2012) (bootlegging).

[25] *See* 18 U.S.C. § 1905 (2012) (penalizing theft of confidential information by government employees); 18 U.S.C. §§ 1961–1968 (2012) (RICO, which enhances punishment for state offenses); 18 U.S.C. § 1030 (2012) (Computer Fraud and Abuse Act, which punishes unlawfully accessing a computer); Carpenter v. United States, 484 U.S. 19, 28 (1987) (holding that the conspiracy to trade on employer's confidential information is within the reach of the mail and wire fraud statutes).

[26] *See* Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 41 (1998). Although approval is no longer needed to initiate prosecutions of theft for private benefit, prosecutions based on an intent to benefit a foreign government must still be approved. *See* DOYLE, *supra* note 15, at 12–13 n.78; U.S. DEP'T. OF JUSTICE, CRIMINAL RESOURCE MANUAL §§ 1122–1123 (2015), http://www.justice.gov/usam/criminal-resource-manual-1122-introduction-economic-espionage-act.

[27] Agreement on Trade-Related Aspects of Intellectual Property Rights, Marrakesh Agreement Establishing the World Trade Organization art. 39, Apr. 15, 1994, 1867 U.N.T.S. 154 [hereinafter TRIPS Agreement]. Article 39.1 protects against "unfair competition." Subsection 2 parallels U.S. trade secret law and requires civil remedies for misappropriating valuable secret information. Subsection 3 protects data exclusivity for information generated to meet market approval of pharmaceutical and agricultural chemical products. This information is undisclosed in only a technical sense (since it is disclosed to the relevant regulatory agency). Unauthorized use of such information is beyond the scope of this paper. In contrast, there are multiple provisions on patents, copyrights, and trademarks.

[28] *Id.* at art. 61 (requiring criminal penalties only for trademark counterfeiting and copyright piracy on a commercial scale).

trade secrecy are profoundly ambiguous. On the one hand, trade secrecy acts as an incentive to innovate and acts as a complement to patent protection in that it is cheaper, can last longer, and covers advances that are not developed enough or sufficiently inventive to qualify for patents. Trade secrecy also allows innovators to transmit technical information to employees, collaborators, investors, fabricators, distributors, regulators, and subsidiaries, safe in the knowledge that if secrets leak, there will be legal recourse to recoup the lost value and retain exclusivity.

But trade secret protection can also act as a substitute for patents. The more it reduces the risk of loss, the greater the temptation to rely on trade secrets instead of patents. Since trade secrecy does not require disclosure of the technical details of inventions, over-zealous trade secret protection can chill innovation, reduce competition, impede entrepreneurship, and interfere with the government's ability to regulate for safety, health, and environmental concerns.[29] Moreover, as one of us has shown, trade secret protection can have a devastating effect on employee mobility and depress salaries in the high technology sector.[30] Anticipating lower salaries, fewer people may be willing to make the very considerable investment in human capital necessary to enter high tech, medical, and scientific fields.

Criminalization further ups the ante. Thus, Christopher Buccafusco and Jonathan Masur argue that the benefits of attaching criminal penalties to intellectual property infringements often outweigh the harm caused by over-deterring legitimate, socially valuable, innovative behavior.[31] Criminalization can be particularly detrimental in the context of trade secret protection. The law includes vague and often circular definitions, which makes it difficult to know exactly what behavior is consid-

---

[29] *See* Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. Rev. 575 (1999); Wesley M. Cohen, Richard R. Nelson & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)*, (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), http://www.nber.org/papers/w7552.pdf; Ivan P.L. Png, Law and Innovation: Evidence from State Trade Secrets Laws 2, 22–23 (June 15, 2012) (unpublished paper), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1755284; Ivan P.L. Png, Secrecy and Patents: Evidence from the Uniform Trade Secrets Act 3, 19 (Dec. 2015) (unpublished paper), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2617266 (demonstrating different effects on different industries).

[30] Orly Lobel, Talent Wants to Be Free: Why We Should Learn to Love Leaks, Raids, and Free Riding 144–50 (2013); Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 Tex. L. Rev. 789 (2015).

[31] Christopher Buccafusco & Jonathan S. Masur, *Innovation and Incarceration: An Economic Analysis of Criminal Intellectual Property Law*, 87 S. Cal. L. Rev. 275, 329–31 (2014) (patent context).

ered illegal; the uncertainty is highly likely to lead to over-deterrence and to chill productive exchanges.[32]

Given widespread concerns about over-protecting trade secrets, the heated rhetoric that currently surrounds economic espionage demands examination. Doubtless, technology has become an increasingly important asset in our modern economy, and the ONCIX Report is surely correct that computer hacking is a growing phenomenon.[33] However, the government's characterization of the problem too broadly expands the notion of what should be considered protectable and what types of activities constitute misappropriation.[34] Through references to "Chinese actors [as] the world's most active and persistent perpetrators"[35] and to "the many Russian immigrants with advanced technical skills who work for leading US companies,"[36] the argument for greater protection appears to derive at least some of its power from xenophobia. Most importantly, the term "espionage"—and the drama of *The Company Man*—conflates private economic interests with national security concerns, and interjects a new dimension to the moral component of innovation policy debates.[37]

In a prescient article published in 2009, Aaron Burstein considered the impact of using innovation laws to protect national security.[38] We essentially ask the converse question: the effect of classifying trade secrecy as a security issue on innovation. Part I provides background on the EEA. Part II examines the rhetoric the government is using to promote its trade secret agenda. Here, we consider whether the FBI is engaging with

---

[32] *Id.* at 331.

[33] ONCIX REPORT, *supra* note 12, at 1, 6–7.

[34] *See, e.g.*, *id.* at 2–3 (classifying as problematic attending trade shows and collecting information from professional journals).

[35] 2014 REPORT, *supra* note 19, at 16.

[36] ONCIX REPORT, *supra* note 12, at 8.

[37] *See, e.g.*, *id.* at 3 (characterizing the loss of economic information as representing "significant costs to US national security"). In contrast, civil trade secret law is thought to reinforce honest business practices. *See also* Shannon Murphy, *How Recent Attempts to Expand Economic Espionage Protection Will Likely Be Futile in Light of Trade Secret Protection Schemes Already Available to U.S. Companies*, MICH. IT LAW., Jan. 2014, at 4, 9, http://www.reising.co/wp-content/uploads/2014/01/Pages-from-Michigan-IT-Lawyer-January-2014-Newsletter.pdf.

[38] Aaron J. Burstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933, 948 (2009) (noting that the more deterrence is provided through criminalization, the less a firm may feel it needs to take action to protect its secrets); *see also* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 860 (2002) (warning that the EEA likely creates a perverse incentive to rely less on patent law while chilling second-generation innovation by controlling knowledge); David Orozco, *Amending the Economic Espionage Act to Require the Disclosure of National Security Related Technology Thefts*, 62 CATH. U. L. REV. 877, 904 (2013) (suggesting that the trade secret protection should be increased and those who do not reveal knowledge of violations should be penalized).

firms (as, for example, producing and disseminating films like *The Company Man*) so the firms will provide the Bureau with leads helpful in ferreting out spies, or whether the security trope emanates from the view that it is in the nation's security interests to protect incumbent innovators from foreign (as well as domestic) competition. Part III investigates the ramifications of the latter view on the interpretation of the EEA and on the innovation environment. First, we examine recent patterns of expansion in investigation, indictments, and convictions under the EEA. Second, we ask about the effects of these recent trends on university research as well as on private market innovation, including entrepreneurship, information flows, and job mobility. Paradoxically, the effort to protect valuable information and retain the United States' leadership position could disrupt information flow, interfere with collaborative efforts, and ultimately undermine the inventive capacity of American innovators. In Part IV, we offer suggestions for reconciling legitimate concerns about national security with the balance that intellectual property law traditionally seeks to strike between incentivizing innovation and ensuring the vibrancy of the creative environment. We conclude that a legal regime aimed at protecting incumbency is not one that can also optimally foster innovation.

I. THE ECONOMIC ESPIONAGE ACT

The EEA was enacted in a period very different from our own. The Cold War had ended; it thus seemed apparent that the espionage profession would collapse as well. As John le Carré—author of *The Spy Who Came in from the Cold*[39]—put it, when the Berlin Wall fell, "I read my own obituary."[40] The master espionage novelist did not, however, fade away. Instead, he found inspiration in the goings-on of the high technology sector.[41] And there was reason to think that spycraft would endure in much the same way: that the future would be one in which countries competed for economic, rather than military, dominance, and espionage agents would move on to stealing valuable industrial and technical information. Concerned, the Senate Select Committee on Intelligence, Judiciary Subcommittee on Terrorism, Technology, and Government Information, and the House Subcommittee on Crime of the Judiciary

[39] JOHN LE CARRÉ, THE SPY WHO CAME IN FROM THE COLD (1963).

[40] Mel Gussow, *In a Plot Far from the Cold, Le Carre Sums Up the Past*, N.Y. TIMES (Dec. 19, 2000), http://www.nytimes.com/2000/12/19/books/in-a-plot-far-from-the-cold-le-carre-sums-up-the-past.html.

[41] Carré's next book challenged the way pharmaceutical companies tested drugs. JOHN LE CARRÉ, THE CONSTANT GARDENER (2001).

Committee considered whether the United States had an effective response.[42] The EEA was the outcome.[43]

The statute defines two crimes. Strictly speaking, "economic espionage" refers to the first: appropriation of a trade secret without authorization, knowing the offense will benefit a foreign government, foreign instrumentality, or foreign agent.[44] The second, "theft of trade secrets," consists of unauthorized appropriation with "intent to convert [the] trade secret . . . to the economic benefit of anyone other than the owner."[45] Apart from the intended beneficiary, the two crimes have similar elements: a subject-matter requirement (the information must qualify as a trade secret), an infringement requirement (the offender must engage in an improper act), intent requirements (intent to benefit for espionage, or to convert for theft), and knowledge requirements (knowledge of appropriating a trade secret for espionage, or knowledge that the act would injure the owner for theft). Notably, both individuals and organizations can be punished, with higher fines and longer terms of imprisonment for economic espionage benefiting foreign governments than for theft leading to private gain.[46] In addition, the prosecutor can demand forfeiture, destruction and restitution,[47] as well as injunctive relief.[48] Because Congress was specifically concerned with improper activity conducted by and for foreign firms and powers, the Act expressly reaches conduct outside the United States in three situations: if an individual offender is a citizen or permanent resident, if an organization is organized under the laws of the United States or a state, or if an act in furtherance of the offense was committed in the United States.[49]

The move to protect trade secrets through federal criminal law troubled intellectual property lawyers because it appeared to alter the relationship between trade secret law and patent law. Patent law requires disclosure of the details of protected inventions and lasts only for a specified term,[50] thereby ensuring that the public has the information necessary to

---

[42] *See* Dreyfuss, *supra* note 26, at 5 & n.13 (citing S. REP. NO. 104-359, at 5 (1996); H.R. REP. NO. 104-788, at 14–16 (1996)). As the FBI's official website once declared, "the Cold War is not over, it has merely moved into a new arena: the global marketplace." *See* Orly Lobel, *America's Hypocritical Approach to Economic Espionage*, FORTUNE (Sept. 24, 2013), http://fortune.com/2013/09/24/americas-hypocritical-approach-to-economic-espionage/.

[43] *See* Kuntz, *supra* note 7, at 904 (explaining why existing statutes were considered inadequate).

[44] 18 U.S.C. § 1831 (2012).

[45] 18 U.S.C. § 1832 (2012).

[46] 18 U.S.C. § 1831(a) (individuals) & (b) (organizations); § 1832(a) & (b) (same).

[47] 18 U.S.C. § 1834 (2012).

[48] 18 U.S.C. § 1836(a) (2012).

[49] 18 U.S.C. § 1837 (2012).

[50] 35 U.S.C. §§ 112 & 154 (2012).

build on a protected advance, to push the frontiers of knowledge forward, and to enjoy the advance itself for free when the period of exclusivity ends. Public documentation of the metes and bounds of inventions also facilitates transactions and permits employees to take unprotected information with them when they change jobs. In contrast, trade secrecy allows innovators to hide what they know from others, including from government regulators, and makes it difficult for employees to alter their positions and put their talents to their highest and best use.

In *Kewanee Oil Co. v. Bicron Corp.*,[51] the Supreme Court upheld a state trade secret law against a preemption challenge. Significantly, it did so because the Court assumed the law would not take knowledge out of the public domain.[52] Further, the justices reasoned that trade secrets were so vulnerable to discovery that, "[t]he possibility that an inventor who believes his invention meets the standards of patentability will sit back, rely on trade secret law . . . is remote indeed."[53] Two important developments took place subsequent to *Kewanee* to ensure the Court's assumptions held true. First, Congress created the Federal Circuit in 1982 because it perceived that patent enforcement had become so weak that inventors were opting instead for trade secret protection.[54] Second, after years of debate, the American Law Institute rebuffed an attempt to amend the Uniform Commercial Code to cover intellectual property licensing. [55] The membership was concerned that improving the enforceability of information contracts would lead to more secrecy and undermine national innovation policy.[56]

---

[51] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

[52] *Id.* at 484–85.

[53] *Id.* at 490.

[54] Federal Courts Improvement Act of 1982, Pub. L. No. 97-164, 96 Stat. 25 (relevant provisions codified as amended in scattered sections of 28 U.S.C.); *see Industrial Innovation and Patent and Copyright Law Amendments: Hearings Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary*, 96th Cong. 574, 575 (1980) (statement of Sidney A. Diamond, Comm'r of Patents and Trademarks).

[55] *See generally* Rochelle Cooper Dreyfuss, *Do You Want to Know a Trade Secret? How Article 2B Will Make Licensing Trade Secrets Easier (but Innovation More Difficult)*, 87 CALIF. L. REV. 191 (1999); Michael Traynor, *The First Restatements and the Vision of the American Law Institute, Then and Now*, 32 S. ILL. U. L.J. 145, 147–49 & 148 n.28 (2007).

[56] *Article 2B Is Withdrawn from UCC and Will Be Promulgated by NCCUSL as a Separate Act*, A.L.I. REP., Spring 1999, at 1; *see, e.g.*, Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111, 114 (1999) ("Article 2B creates a fundamental conflict between the goals of federal and state intellectual property . . . ."); Courtney Lytle Perry, *My Kingdom for a Horse: Reining In Runaway Legislation from Software to Spam*, 11 TEX. WESLEYAN L. REV. 523, 535 (2005) (speaking of "licensing away the public domain"); *see also id.* at 548. That effort was later transformed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) into the Uniform Computer Information Transactions Act, but it too met with considerable resistance and was adopted by only two states. *See* MD. CODE ANN.,

The EEA posed a risk of nullifying these actions. Criminalizing trade secret violations increased deterrence, which made secrets less vulnerable to discovery. In addition, it increased the stakes for ex-employees and their new employers: both could find themselves subject to fines and incarceration if the information used on the new job was deemed to be the previous employer's secret.

To make matters worse, the statute seemingly extended the reach of trade secret protection quite far—arguably, all the way into the public domain. First, it included examples of information that are not mentioned in comparable state laws.[57] More important, while the subject-matter element was cabined by the requirements that the information derive economic value from not being generally known, and that the employer or company take reasonable measures to maintain secrecy,[58] the statute failed to define these terms. Similar concepts in the Uniform Trade Secrets Act (UTSA), the civil trade secret law that most states have adopted, have received disparate interpretations.[59] In some states, trade secret owners must exert considerable effort, and the secret must be absolute. But "reasonable effort" can mean efforts that are inexpensive, which permits even exposed information to be protected in some circumstances.[60] By the same token, while the UTSA could be interpreted to mean that the information is not secret if it is known in business circles,

---

COM. LAW § 22-101 (LexisNexis 2005); VA. CODE ANN. § 59.1-501.1 (2006). A few states even enacted anti-UCITA provisions that made unenforceable agreements that chose the law of UCITA states. *See* Michelle Garcia, *Browsewrap: A Unique Solution to the Slippery Slope of the Clickwrap Conundrum*, 36 CAMPBELL L. REV. 31, 59–60 (2013).

[57] 18 U.S.C. § 1839(3) (2012) defines a trade secret to include "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing." Under the UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 536 (1985), trade secret "means information, including a formula, pattern, compilation, program, device, method, technique, or process."

[58] 18 U.S.C. § 1839(3)(A)–(B). Under the UTSA, the information must "(i) derive[] independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) [be] the subject of efforts that are reasonable under the circumstances to maintain its secrecy." § 1(4).

[59] 14 U.L.A. 536.

[60] *See, e.g.*, E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970) (holding a lawful fly-over to constitute misappropriation); *see also* Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1662–63 (1998) (noting that state laws were not uniform on these issues). *See generally* IP CRIMES MANUAL, *supra* note 11, at 171–73; Robert G. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 46 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011).

the EEA defined "generally known" to mean that the information is known to the general public. Thus, the criminal statute could be viewed as more likely to protect industries from new entrants.[61] Moreover, because the statute required only an intent to injure and not actual injury, and because it also covered attempts and conspiracies, it creates several ways in which taking information that is not actually secret could lead to criminal liability.[62] Analogously, a violation could occur even if there was no real possibility of competitive injury.[63]

Even more problematic was the possibility that the statute would prevent information from ever entering the public domain, either through employees moving to new positions and using their training in their new environment,[64] or through disclosure. Like the definition of trade secret, the EEA provided many examples of unauthorized appropriation that are not listed in the UTSA. These examples include transmitting, communicating, duplicating, and sketching, which suggests that even benign activities, like memorization, can be considered actionable.[65] Further, the

---

[61] *See, e.g.*, United States v. Chung, 659 F.3d 815, 825 (9th Cir. 2011) (noting that courts have interpreted the provision in different ways); IP CRIMES MANUAL, *supra* note 11, at 165; *see also* Moohr, *supra* note 38, at 878–79 (noting the effect of using the general public as a benchmark); *cf.* TRIPS Agreement, *supra* note 27, at art. 39.2 (specifying that the information is not secret if it is accessible within the circles that normally deal with that sort of information).

[62] *See, e.g.*, United States v. Yang, 281 F.3d 534, 544 (6th Cir. 2002) (rejecting an impossibility defense); United States v. Hsu, 155 F.3d 189, 205–06 (3d Cir. 1998) (refusing to permit the defendant to examine whether the information was secret because he was charged with only conspiracy and attempt to steal trade secrets); *see also* IP CRIMES MANUAL, *supra* note 11, at 190 (citing several cases).

[63] *See, e.g.*, United States v. Krumrei, 258 F.3d 535, 537 (6th Cir. 2001) (affirming conviction even though the defendant sold information to a private investigator posing as an agent for a rival firm); IP CRIMES MANUAL, *supra* note 11, at 168.

[64] *See, e.g.*, Gilson, *supra* note 29, at 577–78 (showing that Silicon Valley prospered when employees could easily move from job to job).

[65] Section 1831(a) and (b) consider the following acts actionable if without authorization, a person:

> (1) steals, . . . appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception . . . ;
>
> (2) . . . copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys . . . ;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted . . . ;
>
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy . . . .

18 U.S.C. § 1831. In contrast, the UTSA defines "improper means" as "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy,

statute does not specify defenses (apart from certain governmental activity)[66] or define what constitutes a "proper means" of acquisition.[67] Thus, it leaves the status of reverse engineering—a crucially important way in which secrecy is lost—unclear.[68] Finally, unlike in civil actions, where injunctive relief usually lasts only as long as the information is secret or would be discovered, [69] the EEA requires only that any injunction issued be "appropriate."[70]

Despite these reservations, the EEA went into effect. However, Congress slowed enforcement by requiring that every prosecution during the first five years obtain specific approval from the Attorney General's office.[71] Even afterwards, prosecutors proceeded gingerly, careful to maintain the long-standing balance between existing state trade secret laws and these newly enacted federal measures.[72] Initially, Government attorneys were instructed to focus on specific pieces of information and avoid prosecutions that raised questions about an employee's training or the ability to reverse-engineer.[73] For example, even though the Justice Department concluded that memorization can be an unlawful means of appropriation, it differentiated between material committed to memory and "knowledge, skills, or abilities."[74]

---

or espionage through electronic or other means." 14 U.L.A. 536; *see also* Dreyfuss, *supra* note 26, at 14. The Department of Justice has concluded that memorization is a method of misappropriation. *See* IP CRIMES MANUAL, *supra* note 11, at 175–76.

[66] 18 U.S.C. § 1833 (2012).

[67] 18 U.S.C. § 1839(3)(B) (2012).

[68] *See* James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 195 (1997); Craig L. Uhrich, *The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 169 (2001), Burdens of proof on issues like reverse engineering are similarly under-defined. *Cf.* Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015) (addressing the question whether fair use is an affirmative defense or must be disproved by the copyright holder).

[69] *See generally* Christopher A. Cotropia, Note, *Post-Expiration Patent Injunctions*, 7 TEX. INTELL. PROP. L.J. 105 (1998).

[70] 18 U.S.C. § 1836(a) (2012).

[71] *See* Dreyfuss, *supra* note 26, at 41.

[72] Private conversation with New York Assistant U.S. Attorney; *see* IP CRIMES MANUAL, *supra* note 11, at 161–62 (noting the relevance of civil case law).

[73] IP CRIMES MANUAL, *supra* note 11, at 162. The Manual does, however, note that for attempts and conspiracies, there is no need to prove the information was actually secret. *Id.* at 164.

[74] *Id.* at 176, 191 (citing United States v. Shiah, No. SA CR 06-92, at 38–39 (C.D. Cal. Feb. 19, 2008), http://court.cacd.uscourts.gov/cacd/recentpubop.nsf/0/37d207fcb9587a30882573f400620823/$FILE/SACR06-92DOC.pdf). Before changing jobs, the defendant downloaded 4,700 files but successfully defended on the ground this was part of his "toolkit" of information he had developed during the course of his career.

The statute as originally drafted included several important limitations. It provided that a trade secret must be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[75] Thus, the Act arguably targeted only situations where the information was actually embedded in a product and caused real competitive harm. In addition, the scienter elements could act as a limit. For economic espionage, the statute provided that the prosecutor must show the defendant intended or knew the offense would benefit a foreign government, and knew that it was misappropriating a trade secret.[76] On the theft side, the requirements were an intent to convert a secret for the economic benefit of another, knowledge the act would injure the owner, and knowledge that the defendant was appropriating a trade secret.[77] Depending on how "trade secret" and "appropriation" were interpreted, these requirements potentially had significant bite.[78]

Kewanee also arguably exerted restraint. The case was part of a series of Supreme Court decisions on preemption that were often unclear as to whether the problem was the Supremacy Clause[79]—state interference with federal policy (in which case, Congress was free to make a change in the balance between trade secrecy and patenting)—or whether stronger trade secret protection was inconsistent with the Copyright and Patent Clause of the Constitution.[80] Since there was authority for the view that Congress could not end-run limits imposed on one constitutional power by enacting law under another authority,[81] the EEA arguably had to be interpreted in ways that avoided interfering with a constitutionally based balance between trade secrecy and patent law.[82] Indeed, at the 16-year mark, Peter Toren, former prosecutor in the Computer Crime and Intel-

---

[75] George J. Moscarino & Michael R. Shumaker, *Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response*, 16 DICK. J. INT'L L. 597, 612 (1998) (citing § 18 U.S.C. 1832(a) as it read at the time of enactment).

[76] 18 U.S.C. § 1831(a) (2012).

[77] 18 U.S.C. § 1832(a) (2012).

[78] *See* Dreyfuss, *supra* note 26, at 21–24; Moohr, *supra* note 38, at 907.

[79] U.S. CONST. art. VI, cl. 2.

[80] U.S. CONST. art. I, § 8, cl. 8; *see, e.g.*, Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 143–44 (1989); *cf.* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344–45 (1991) (expressing shifting views on whether protecting facts is preempted by copyright law or the Copyright Clause); Graham v. John Deere Co., 383 U.S. 1, 5 (1966) (noting that the Copyright Clause is a "grant of power and a limitation"). *See generally* Paul J. Heald & Suzanna Sherry, *Implied Limits on the Legislative Power: The Intellectual Property Clause as an Absolute Constraint on Congress*, 2000 U. ILL. L. REV. 1119.

[81] *See* Ry. Execs.' Ass'n v. Gibbons, 455 U.S. 457, 468 (1982) (preventing Congress from avoiding limits in the Bankruptcy clause, U.S. CONST. art. I, § 8, cl. 4).

[82] *See, e.g.*, IP CRIMES MANUAL, *supra* note 11, at 199 (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) on the question whether reverse engineering is a defense).

lectual Property Division of the Justice Department, analyzing all the cases that had led to a successful indictment, concluded as follows:

> At the time the EEA was enacted in 1996, there was concern raised that the government would become involved in the prosecution of not only garden-variety theft of trade secret cases, but would prosecute cases that did not even rise to the level of civil trade secret violations.
>
> Contrary to this claim, the cases that the government has prosecuted generally involve allegations of serious losses to the victims caused by the trade secret thefts. Further, while the pace of prosecutions has increased slightly in recent years, the relatively limited number of prosecutions also suggests that the government is being extremely selective in the number and type of cases it investigates and prosecutes.[83]

II. THE RHETORIC OF PROTECTION

Psychic spies from China
Try to steal your mind's elation
–Californication, Red Hot Chili Peppers

Against this backdrop, the recent enthusiasm for trade secret criminalization is curious. Consider *The Company Man*.[84] The film depicts how insidiously those intending to steal technology operate. The Chinese government's goal appeared to be admirable: the viewer is initially sympathetic to its desire to protect homes from fire. Responsive to this concern, a company contacts a U.S. firm specializing in insulation. The first meeting includes a textbook negotiation in which the parties discuss the choice between shipping finished product or entering into a joint manufacturing venture in China. Dealings with the engineer are equally familiar: would he go to China or work from his home in the United States? Only slowly do matters go awry. We learn that one of the principals was formerly in the People's Liberation Army; a member of the Chinese negotiating team tries to tap into the U.S. firm's computer; eventually, the engineer realizes he doesn't really need to *work* from home; he can earn his "salary" by simply disclosing the firm's technology. The film, in short, reveals the methods used by those who wish to learn American secrets and describes clues a firm should look out for as it enters into business relationships in China. Further, the film identifies the characteristics of employees vulnerable to co-opting: the engineer needed money to send his daughter to Princeton; he was frustrated by the firm's failure to promote him.

---

[83] Toren, *supra* note 9.

[84] *See supra* note 1.

But why did the FBI make the film? There are many crimes—insider trading, conspiracies to restrain trade, corruption, blackmail—where associations begin innocently, proceed incrementally to illegality, and ultimately inflict significant harm.[85] Thus, it would be equally helpful for the FBI to make films that illustrate the early warning signs of other white-collar crimes. Yet the government does not usually spend taxpayer money in this way. Why here? The last frame of the film is suggestive: "To report suspicious activity, contact your local FBI office, or go to https://tips.fbi.gov." In other words, not only does the FBI want to help U.S. firms protect their technology, it also wants U.S. firms to help the FBI—specifically, the division of the FBI that made the film, the Counterintelligence Division, Counterespionage Section.[86]

Perhaps, then, one goal of the film is to enlist the private interests of U.S. firms to supply the FBI with leads to the location of infiltrators. Knowing who is present in the United States, identifying associates, finding patterns in their communications, and learning of foreigners trained in computer science and other technical fields are arguably important ways to keep track of potential hackers, bomb makers, terrorists, and such. The government need not follow every tip or prosecute every individual to benefit from encouraging the high tech sector to be more vigilant about spotting intruders. Informing firms that it is there to help and reassuring them that the FBI will protect their secrets may be critical to coaxing the victims of theft to abandon concerns about turning over their cases and information about their critical technology to government prosecutors.

A review of other government materials suggests, however, that the emphasis on economic espionage is not meant merely to ferret out terrorists. Rather, it appears that the government's view of trade secret misappropriation has changed. Economic espionage is no longer seen as *supplanting* military espionage; now, economic espionage *is* military espionage. In a 2000 Congressional hearing of the Subcommittee on International Economic Policy and Trade, talks began with the following statement:

> The past decade has brought profound changes, yet some of the characteristics of the old world order continue to live on today, with some of the darker impulses of yesteryears adapting to fit a new time and a new set of standards and requirements.

---

[85] *See, e.g.*, Tamar Lewin, *Young, Eager and Indicted*, N.Y. TIMES, June 2, 1986, at D1 (describing an SEC investigation of insider trading begun over Sabbath dinners).

[86] In the view of Bill Evanina, head of the National Counterintelligence and Security Center, many of the tools used to counter economic espionage are the same tools used to target and track terrorists. Wesley Bruer, *FBI Sees Chinese Involvement amid Sharp Rise in Economic Espionage Cases*, CNN (July 24, 2015), http://edition.cnn.com/2015/07/24/politics/fbi-economic-espionage/.

> The front line is no longer the one which divides East and West, but the one defined by technological innovations. The battle lines lie in research and development. Resources designed and previously used exclusively for military intelligence gathering are now being expanded to gather intelligence on mergers, investments and other financial transactions. The generals are being replaced with CEOs, and the bottom line is not ideological, but financial.[87]

The Congressional hearing also included an explanation by the FBI's Deputy Assistant Director for Counterintelligence as to why economic espionage against the United States had expanded. First, the collapse of the Soviet Union, which meant that "[other countries] found themselves looking around and saying look, we have got to redefine what is our national security. It is no longer aligning ourselves with the Soviet Union or the west. It is we have to have a piece of the economic pie."[88] Second, military allies "are now aggressive economic competitors" who also want to gain a "piece of the pie."[89] And third, "rapid globalization of the world economy defines national security not so much in how many tanks you have deployed or how many soldiers you have on the field necessarily, but instead their strength is measured in terms of the nation's economic capability."[90] The speaker concluded his comments with the words "national security equals economic security."[91]

A decade later, the equation between military and financial interests is commonplace. The 2012 Targeting Analysis begins with the statement that U.S. national security depends on thwarting persistent attacks on "U.S. technology, intellectual property, trade secrets, and proprietary information."[92] When the 2013 Administration Strategy Report emphasizes foreign competitors "with ties to foreign governments," it refers to perpetrators as "spies."[93] It notes that one focus of the FBI's outreach is defense contractors and features the important role played by the Department of Defense.[94] The Report also highlights seven cases, all involving key geopolitical adversaries: in six, the perpetrator is Chinese; in the other, a Rus-

---

[87] *Corporate and Industrial Espionage and Their Effects on American Competitiveness: Hearing Before the Subcomm. on Int'l Econ. Policy & Trade of the H. Comm. on Int'l Relations*, 106th Cong. 1 (2000) [hereinafter *Industrial Espionage Hearing*] (statement of Rep. Ileana Ros-Lehniten, Chairperson, Subcomm. on Int'l Econ. Policy & Trade), http://www.gpo.gov/fdsys/pkg/CHRG-106hhrg68684/html/CHRG-106hhrg68684.htm.

[88] *Id.* at 4 (statement of Sheila W. Horan, Deputy Ass't Dir. for Counter Intelligence, Nat'l Security Div., FBI).

[89] *Id.*

[90] *Id.*

[91] *Id.* at 5.

[92] TARGETING ANALYSIS, *supra* note 13, at 5.

[93] STRATEGY REPORT, *supra* note 9, at 1 & n.1.

[94] *Id.* at 9 n.9.

sian.[95] Further, it includes an annex summarizing the 20 cases pursued from January 2009 to January 2013. All but three involve secrets intended for use in China.[96]

Interestingly, the FBI treats the tradecraft involved in misappropriation as equivalent to that used in traditional espionage. Thus, it is not insignificant that the FBI made a companion to *The Company Man. Game of Pawns*[97] tells the story of another slow seduction, this time of an American student who is encouraged by China to obtain a position with the CIA. In other materials, the FBI even warns businesses about the classic "honey pot" stratagem, advising firms that Asian women are often bait for innocent white American men who can't hold their liquor. Once intoxicated, these men can easily be taken to hotel rooms where they can be seduced into revealing sensitive information and their computers can be hacked. In one trade secret summit in California, an FBI special agent advised companies and inside counsel against sending men susceptible to the honey pot on business travel to China. Instead, the agent suggested that when possible, it is advisable to send women rather than men to meetings in China because women are less likely to be tempted.[98]

In one way, this is unexceptional. Hacking, after all, is a form of physical attack ("cyberwarfare") as it can sabotage important infrastructure such as power grids, air traffic control, and financial institutions.[99]

---

[95] *Id.* at 4, 5, 7, 9, 10, 12. The Report mentions no domestic cases. Annex B to the Report lists 20 cases prosecuted from January 2009 to January 2013. One involves South Korea, one India, one Israel; the rest are about secrets intended for use in China. *Id.* at annex B.

[96] *Id.* at annex B. The other three involve South Korea, India, and Israel. Toren's analysis of the 124 cases brought before September 2012 show that the overwhelming majority involved China. The rest involved India, the Dominican Republic, South Korea, South Africa, Israel, and Japan. *See* Toren, *supra* note 9.

[97] FBI, *Game of Pawns*, YOUTUBE (Apr. 14, 2014) https://www.youtube.com/watch?v=R8xlUNK4JHQ. For additional FBI short films, *see Dramatic Narrative*, *supra* note 1.

[98] Nicholas Shenkin, FBI, Presentation at the Am. Intellectual Property Law Ass'n 2014 Trade Secret Law Summit (Dec. 4, 2014). This is, of course, a well-known technique for real espionage. *See, e.g.*, JAMES P. WELCH, BEHIND CLOSED DOORS: SEX, LOVE, AND ESPIONAGE: THE HONEYPOT PHENOMENON (2012), http://www.academia.edu/2577766/Behind_Closed_Doors_Sex_Love_and_Espionage_The_Honeypot_Phenomenon (describing its use by the KGB, the Stasi, North Korea, and China); Phillip Knightley, *The History of the Honey Trap*, FOREIGN POL'Y (Mar. 12, 2010), http://foreignpolicy.com/2010/03/12/the-history-of-the-honey-trap/; Ray Semko, *China #1 Country for 'Sexpionage,'* DICE MAN: BLOG (Dec. 2, 2011), http://www.raysemko.com/2011/12/02/china-1-country-for-sexpionage/.

[99] *See, e.g.*, David E. Sanger, *In Cyberspace, New Cold War*, N.Y. TIMES (Feb. 24, 2013), http://www.nytimes.com/2013/02/25/world/asia/us-confronts-cyber-cold-war-with-china.html; Damian Paletta, *When Does a Hack Become an Act of War?*, WALL ST. J. (June 13, 2015), http://www.wsj.com/articles/when-does-a-hack-become-an-act-of-war-1434189601.

Moreover, many of the technologies susceptible to theft are important in combat. Insulation, for example, while useful in preventing residential fires of the type depicted in the first scene of the film, is also matériel: equipment used to protect the military during attacks and in battle. Thus, the ONCIX Report lists, as targets of foreign interest, military technologies and "dual-use technologies" (commercial technologies, like insulation, that also have military uses).[100] It specifically points out the persistent, extensive, and sophisticated efforts of intelligence services in China and Russia.[101] The Administration Strategy Report highlights a case where a Motorola software engineer was intercepted while on her way to China, where she planned to turn over mobile-telecommunications technology to the Chinese Army.[102] In this sense, the effort to curb theft is part of a larger program, one that also includes export control regulations, which were similarly adopted during the Cold War to prevent the acquisition of sensitive information by foreign powers.[103]

But increasing the protection of military materials is not all that the national security trope appears to signify. Unlike export control regulations, which attempt to distinguish among technologies and accord a level of scrutiny that is proportionate to the significance of the technology to military objectives,[104] the EEA and its accompanying government reports treat all information in the same way. For example, the ONCIX Report does not stop at dual-use technologies; it also discusses information and communications technology (ICT), including computerization of manufacturing, clean-air technologies, advanced manufacturing technologies (such as nanotechnology), pharmaceuticals, agricultural technology, and information about business deals.[105] These are described not in terms of their military use, but rather in regard to their civilian applications.[106] Thus, they are of interest because the areas are "expected to experience surges in investment," are among the "fastest growing investment sectors," or will "boost industrial competitiveness."[107] According to the Report, healthcare services and medical devices are a focus because they represent "two of the five fastest growing international investment

---

[100] ONCIX REPORT, *supra* note 12, at 8.

[101] *Id.* at 5.

[102] STRATEGY REPORT, *supra* note 9, at 10.

[103] 22 U.S.C. § 2778 (2012); *see* TARGETING ANALYSIS, *supra* note 13, at 28. *See generally* Burstein, *supra* note 38, at 952–59 (describing classification, export controls, and controls on the acquisition of a domestic entity by a foreign government as other efforts to protect national security interests in high tech information); David R. Fitzgerald, *Leaving the Back Door Open: How Export Control Reform's Deregulation May Harm America's Security*, 15 N.C. J.L. & TECH. 65, 68–71 (2014).

[104] *See generally* Fitzgerald, *supra* note 103, at 71–78.

[105] ONCIX REPORT, *supra* note 12, at 8–10.

[106] *Id.* at 9–10.

[107] *Id.* at 8.

sectors."[108] Indeed, it is difficult to see how information about business deals has any value other than for commercial use.

Nor is the government interested only in standard forms of theft. The ONCIX Report, for example, contains a broad list of activities the United States considers "methods of economic espionage."[109] It includes engagement at conferences, conventions, and trade shows; entering into joint research projects; and exploitation of open source information, such as "information . . . available in professional journals, social networking and other public websites, and the media."[110] Academia, where cutting edge information is routinely exchanged, is a particular locus of concern. The Targeting Analysis discusses, as a method used to collect information, "academic solicitation," including requests to join scientific review boards, requests to study or consult with faculty members, or to be admitted to academic institutions.[111] Two of the seven examples highlighted in the Administration Strategic Report involve research for university use.[112] The ONCIX Report describes academic institutions as a target of espionage and a focus of FBI awareness programs,[113] and includes a claim that Chinese students take home secret scientific information from the universities where they study.[114] Moreover, the Report uses the yearly expenditures of the National Science Foundation (NSF) as one measure of the value of information the government regards as "most vulnerable to economic espionage"[115]—even though the NSF awards much of that funding to basic scientific research, with the intent that grantees publish their results.[116]

The Company Man is thus a piece of a larger strategy to inform the private sector about "[t]he number and identity of foreign governments involved in trade secret misappropriation" and the methods used in the espionage activity.[117] Indeed, the FBI has already used it in over 1,300 briefings with various industry leaders to demonstrate the global threat of

---

[108] *Id.* at 9.

[109] *Id.* at 2.

[110] *Id.* at 2–3.

[111] TARGETING ANALYSIS, *supra* note 13, at 11 fig.4.

[112] STRATEGY REPORT, *supra* note 9, at 5, 7; *see also id.* at 9 (noting an FBI focus on "cleared defense contractors, universities, hospitals, high science companies, and emerging technology firms" (footnote omitted)).

[113] ONCIX REPORT, *supra* note 12, at 1, A-2.

[114] *Id.* at B-3.

[115] *Id.* at 4.

[116] *See* NAT'L SCI. FOUND., GRANT POLICY MANUAL § 741 (July 1, 2005), http://www.nsf.gov/pubs/manuals/gpm05_131/gpm05_131.pdf ("NSF advocates and encourages open scientific and engineering communication. NSF expects significant findings from research it supports to be promptly submitted for publication . . . ."); *see also Introduction/NSF Mission*, NAT'L SCI. FOUND., https://www.nsf.gov/policies/egov_inventory.jsp.

[117] STRATEGY REPORT, *supra* note 9, at 8.

economic espionage and the infamous "blundering Chinese executives" hungry for American trade secrets.[118] As another part of this effort, the U.S. Patent and Trademark Office and International Trade Administration utilize "current 'road show' trainings to provide forums to educate the private sector, particularly small- and medium-sized businesses, regarding the economic implications of corporate and state sponsored trade secret theft."[119] The FBI is rather creative in its educational efforts. Beyond film, the FBI website includes interviews and podcasts meant to educate businesses about contemporary threats. In one such podcast an FBI agent is interviewed about the first economic espionage trial in U.S. history. Special Agent Moberly begins, "[t]he stealing of our trade secrets from our companies and giving those secrets to any foreign government inflicts billions of dollars of loss to our nation and our economy. That is a national security issue."[120] The interviewer then jumps in: "I'm Mollie Halpern of the FBI, and this is Gotcha. The 2010 case put Chinese-born and U.S. naturalized citizen Dongfan 'Greg' Chung behind bars for nearly 16 years."[121]

The focus on China (and to a lesser extent on Russia)—as opposed to close allies also well known for theft[122]—is telling. In part, it may be that China is the prime perpetrator. Thus, a recent, in-house, FBI study found that, while only half of the 165 private companies involved claimed to be victimized, of those that did, 95% of the theft involved perpetrators with ties to the Chinese government.[123] But China is not just "the yellow

---

[118] Elias Groll, *FBI Rolls Out Red Scare Film to Highlight Threat of Economic Espionage*, FOREIGN POL'Y (July 23, 2015), https://foreignpolicy.com/2015/07/23/fbi-rolls-out-red-scare-film-to-highlight-threat-of-economic-espionage/.

[119] *White House Unveils New Strategy to Mitigate Theft of U.S. Trade Secrets*, HKTDC (Mar. 8, 2013), http://hkmb.hktdc.com/en/1X09SAES/hktdc-research/White-House-Unveils-New-Strategy-to-Mitigate-Theft-of-US-Trade-Secrets.

[120] *Dongfan "Greg" Chung*, FBI: PODCASTS & RADIO (May 11, 2012), https://www.fbi.gov/news/podcasts/gotcha/dongfan-greg-chung.mp3/view.

[121] *Id.*

[122] *See, e.g.*, U.S. GEN. ACCOUNTING OFF., GAO/NSIAD-96-64, DEFENSE INDUSTRIAL SECURITY: WEAKNESSES IN U.S. SECURITY ARRANGEMENTS WITH FOREIGN-OWNED DEFENSE CONTRACTORS 2 (1996) (noting that "some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means"); Arthur Bright, *France Upbraids US for Spying on Its Leaders. Should It Be Throwing Stones?*, CHRISTIAN SCI. MONITOR (June 24, 2015), http://www.csmonitor.com/World/Security-Watch/terrorism-security/2015/0624/France-upbraids-US-for-spying-on-its-leaders.-Should-it-be-throwing-stones-video ("France's complaints rang somewhat hollow, due to its own long history of espionage against allies—particularly corporate interests and business."). There have not been many purely domestic cases either, although the St. Louis Cardinals are currently under investigation. *See* Michael S. Schmidt, *Cardinals Investigated for Hacking into Astros' Database*, N.Y. TIMES (June 16, 2015), http://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html.

[123] Bruer, *supra* note 86.

peril"[124] in a political or military sense. It is a large, emerging economy, recognized to be developing a major presence in the high technology sector.[125] It is investing billions of dollars in creating laboratories, training scientists, and engaging in research and development.[126] Patent applications by Chinese inventors are soaring.[127] Unlike time-honored rivals like France or Germany, the technological potential in these countries is unknowable. The ONCIX report characterizes the problem as follows:

> China and Russia will remain aggressive and capable collectors of sensitive [U.S.] economic information and technologies, particularly in cyberspace. Both will almost certainly continue to deploy significant resources and a wide array of tactics to acquire this information from [U.S.] sources, motivated by the desire to achieve economic, strategic, and military parity with the United States.

---

[124] Keith Aoki, *The Yellow Pacific: Transnational Identities, Diasporic Racialization, and Myth(s) of the "Asian Century,"* 44 U.C. DAVIS L. REV. 897, 908 n.34 (2011).

[125] *See* THE GLOBAL INNOVATION INDEX 2015: EFFECTIVE INNOVATION POLICIES FOR DEVELOPMENT 10 (Soumitra Dutta, Bruno Lanvin & Sacha Wunsch-Vincent eds., 2015), https://www.globalinnovationindex.org/userfiles/file/reportpdf/GII-2015-v5.pdf (noting that China is now "on the heels of rich countries"); *see also* Peter K. Yu, *Intellectual Property, Economic Development, and the China Puzzle*, *in* INTELLECTUAL PROPERTY, TRADE AND DEVELOPMENT: STRATEGIES TO OPTIMIZE ECONOMIC DEVELOPMENT IN A TRIPS-PLUS ERA 173, 198 (Daniel J. Gervais ed., 2007); Carl J. Dahlman, *China and India: Emerging Technological Powers*, ISSUES SCI. & TECH., Spring 2007, at 45. According to the most recent PriceWaterhouseCoopers report on global economic power, "China will clearly be the largest economy by 2030, but its growth rate is likely to revert to the global average in the long run." *Shift of Global Economic Power to Emerging Economies Set to Continue, Despite Marked Slowdown in China After 2020*, PRICEWATERHOUSECOOPERS (Feb. 10, 2015), http://press.pwc.com/global/shift-of-global-economic-power-to-emerging-economies-set-to-continue-dispite-marked-slowdown-in-chin/s/7bfcf11d-0804-4fd3-a469-3ef5517f0edb. These shifts also mean an ambivalence by partners to produce in China. John J. Metzler, *PRC's Li Visits France, but Business Interests Are Motive*, CHINA POST (July 11, 2015), http://www.chinapost.com.tw/commentary/the-china-post/john-metzler/2015/07/11/440395/PRCs-Li.htm ("Though Airbus is enchanted with Chinese market possibilities, the question of industrial espionage at the Tianjin mega facilities as well as the very real possibility that Chinese-produced Airbus jets will eventually replace workers at the firm's European facilities in France and Germany remains a nervous concern.").

[126] *See, e.g.*, Didi Kirsten Tatlow, *A Scientific Ethical Divide Between China and West*, N.Y. TIMES (June 29, 2015), http://www.nytimes.com/2015/06/30/science/a-scientific-ethical-divide-between-china-and-west.html; Peter K. Yu, *Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats*, 2015 CARDOZO L. REV. DE NOVO 130, 139, http://www.cardozolawreview.com/content/denovo/YU.36.denovo.symposium.pdf (noting that since 2012, more than two million patent applications have been filed annually in the Chinese patent office).

[127] *See US and China Drive International Patent Filing Growth in Record-Setting Year*, WORLD INTELL. PROP. ORG. (Mar. 13, 2014), http://www.wipo.int/pressroom/en/articles/2014/article_0002.html.

> *China will continue to be driven by its longstanding policy of "catching up fast and surpassing" Western powers.*[128]

It is therefore not surprising that the FBI website reaches out to the American public with a wealth of information and warnings:

> The FBI seeks your help in safeguarding our Nation's secrets!
>
> Our Nation's secrets are in jeopardy, the same secrets that make your company profitable. The FBI estimates billions of U.S. dollars are lost to foreign competitors every year. These foreign competitors deliberately target economic intelligence in advanced technologies and flourishing U.S. industries.
>
> Foreign competitors operate under three categories to create an elaborate network of spies:
>
> 1. Aggressively target present and former foreign nationals working for US companies and research institutions;
> 2. Recruit and perform technical operations to include bribery, discreet theft, dumpster diving (in search of discarded trade secrets) and wiretapping; and,
> 3. Establish seemingly innocent business relationships between foreign companies and US industries to gather economic intelligence including proprietary information.
>
> In an effort to safeguard our nation's economic secrets, the Economic Espionage Act (EEA) was signed into law on October 11, 1996.[129]

In fact, "the FBI Director has designated espionage as the FBI's number two priority—second only to terrorism."[130] In 2010, the FBI's Counterintelligence Division created the Economic Espionage Unit, a specialized group focused solely on prosecuting cases under the Economic Espionage Act and dedicated to countering the economic espionage threat through training and outreach materials, participating in conferences, visiting private industry, working with the law enforcement and intelligence community on requirement issues, and providing classified and unclassified presentations.[131] According to the FBI, "from FY [fiscal year] 2009 to the end of FY 2013, the number of economic espionage and theft of trade secrets cases overseen by the unit increased by more than 60 percent," and "[e]conomic espionage and theft of trade secrets

---

[128] ONCIX REPORT, *supra* note 12, at 7 (emphasis added).

[129] *Economic Espionage: Protecting America's Trade Secrets*, FBI, https://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage-1.

[130] *Id.*

[131] *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 114th Cong. 1 (2014) [hereinafter Coleman] (statement of Randall C. Coleman, Ass't Dir., Counterintell. Div., FBI); *Economic Espionage*, *supra* note 129.

represent the largest growth area among the traditional espionage cases overseen by CD's Counterespionage Section."[132] Assistant Director of the FBI's Counterintelligence Division, Randall Coleman, summed things up in his testimony before the Senate: "By obtaining what it needs illegally, China avoids the expense and difficulty of basic research and unique product development."[133]

Two new Congressional initiatives specifically target China. House Resolution 643, entitled *Calling for Further Defense Against the People's Republic of China's State-Sponsored Cyber-Enabled Theft of Trade Secrets, Including by the People's Liberation Army*, describes the need for aggressively implementing and coordinating strategies to mitigate trade secret theft by China.[134] It recommends more investigations and prosecutions by the Department of Justice, and it asks the FBI and the Department of Homeland Security to expand warnings to U.S. companies about the large array of tools used by actors originating in the People's Republic of China to elicit trade secrets.[135] In addition, the resolution demands that the Department of Defense restrict military-to-military contacts with China.[136] Similarly, a new bill, the *Chinese Communist Economic Espionage Sanctions Act*, calls on Congress to condemn the Chinese Communist Party and the Chinese government for economic and cyber-espionage against the United States.[137] The Act would deny persons and Chinese entities involved in espionage entry into the United States and freeze their assets.[138] All transactions in property and property interests of a "covered Chinese state-owned enterprise" or a person who is a member of the board of directors, an executive officer, or a senior official of such enterprise, would be blocked or prohibited if those property and property interests are in the United States, come within the United States, or are within the possession or control of a U.S. person.[139] The Act would further make an alien ineligible for a visa and for U.S. admission if the alien is a member of the board of directors, an executive officer, or a senior official of a covered Chinese state-owned enterprise; and the act would direct the Secretary of State to

---

[132] Coleman, *supra* note 131, at 2.

[133] *Id.*

[134] H.R. 643, 113th Cong. (2014).

[135] *Id.*

[136] *Id.*

[137] H.R. 5103, 113th Cong. § 3 (2014).

[138] *Id.* §§ 4, 5.

[139] The legislation defines "covered Chinese state-owned enterprise" to mean an enterprise that "(A) is organized under the laws of the People's Republic of China, including a foreign branch of such enterprise; and (B) is owned or controlled by the Government of the People's Republic of China or the Chinese Communist Party." *Id.* § 4(d).

revoke the visa or other documentation of any alien who would be ineligible to receive the visa or documentation.[140]

While not as often mentioned as the Chinese, Russians are also the subject of the discourse on trade secret theft. The publicity surrounding the prosecution of Sergey Aleynikov is particularly suggestive of the fear that foreigners will destroy the technological dominance of the United States. His case is heavily featured in the Administration Strategic Report, where he is described as having transferred "extremely valuable proprietary computer code" used in high-frequency trading to an external server at the time he left a job at Goldman Sachs to go work for a rival.[141] He was prosecuted twice; both times, he was convicted and both times, the conviction was overturned. In federal court, the conviction (to which an eight-year sentence was attached) was thrown out because the prosecutor had failed to show that the source code was embedded in a product used in commerce, as required by the EEA.[142] A subsequent prosecution under state law ended similarly. The jury's conviction for "unlawful use of secret scientific material" was overturned because the presiding judge did not believe that Aleynikov's actions fit the requirements of New York law that the material taken be "tangible," or that he had the intent to appropriate something of value.[143] Furthermore, the judge noted that the jury faced "an unusually difficult task" applying the law to the facts of the case.[144]

It is no wonder the jury might have been confused: Aleynikov left with 32 megabytes from a platform that consisted of an estimated 1 gigabyte of code, none of which included Goldman's trading strategies, and some of which was open source and available on the internet. Furthermore, the evidence suggested that it was part of a system so archaic, the material held little interest to his new employer.[145] Nonetheless, the coverage of the case has been pervasive and virtually always stresses Aleynikov's obviously Russian name (as in the Administration Strategic Report) and sometimes, his appearance. According to Michael Lewis, "in a lineup of people chosen randomly from the streets, he is the guy most likely to be identified as a Russian spy."[146] And yet, Aleynikov immigrated to the United States in 1990, was in the United States for years before joining

---

[140] *Id.* § 5(a)–(b). Immigration-related consequences were similarly proposed in the *Cyber Economic Espionage Accountability Act. See* H.R. 2281, 113th Cong. § 4 (2013).

[141] STRATEGY REPORT, *supra* note 9.

[142] United States v. Aleynikov, 676 F.3d 71, 82 (2d Cir. 2012).

[143] People v. Aleynikov, 15 N.Y.S.3d 587, 627, 630 (Sup. Ct. 2015).

[144] *Id.* at 627; *see also* Matthew Goldstein, *Conviction of Former Goldman Sachs Programmer Is Overturned*, N.Y. TIMES (Jul. 6, 2015), http://nyti.ms/1LNNts4.

[145] MICHAEL LEWIS, FLASHBOYS: A WALL STREET REVOLT 136–39 (2015); Michael Lewis, *Did Goldman Sachs Overstep in Criminally Charging Its Ex-Programmer?*, VANITY FAIR (Aug. 31, 2013), http://www.vanityfair.com/news/2013/09/michael-lewis-goldman-sachs-programmer.

[146] Lewis, *supra* note 145, at 5.

Goldman, held American citizenship, and was leaving Goldman to join another U.S. based company. But as the quotation above shows, the FBI's view is that the risk of espionage stems from "present and *former* foreign nationals."[147]

The message, in short, is that foreign-born scientists are dangerous and that foreign interest in U.S. technology is an existential threat. Government materials warn against diminishing "U.S. export prospects around the globe" and putting "American jobs at risk."[148] The Administration Strategy Report quotes President Obama: "We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy. . . . Congress should make sure that no foreign company has an advantage over American manufacturing."[149] When the Foreign and Economic Espionage Penalty Enhancement Act of 2012 was signed into law, increasing the "criminal penalties for economic espionage and direct[ing] the Sentencing commission to consider increasing offense levels for trade secret crimes," the administration explained the passage of the law as "an important step in ensuring that penalties are commensurate with the economic harm inflicted on trade secret owners."[150] As the Administration Strategy Report puts it: "Trade secret theft . . . undermines national security[] and places the security of the U.S. economy in jeopardy."[151]

In the final analysis, the EEA is no longer merely a tool of innovation policy—a technique for protecting short-term exclusivity in order to encourage *future* investments in innovation. Instead, it is a vital part of an initiative aimed at protecting the United States' *current* technological dominance. Hence the government's preference that the tech sector compartmentalize access to trade secrets, even intimating that U.S. firms should approach conferences, conventions, trade shows, and even open-publication and students warily, despite the potential loss of important information exchanges.[152] (This emphasis may also explain why the government is using Special 301 actions to pressure other countries to adopt trade secret laws, including making trade secret protection a "priority issue" in bilateral and regional agreements, entering into cooperative arrangements with foreign governments to enhance investigation, and proposing a private federal cause of action for industrial espionage.)[153]

---

[147] *Economic Espionage*, *supra* note 129 (emphasis added).

[148] STRATEGY REPORT, *supra* note 9, at 1; *see also* TARGETING ANALYSIS, *supra* note 13, at 5.

[149] STRATEGY REPORT, *supra* note 9, at 1, 11.

[150] *Id.* at 11.

[151] *Id.* at 1.

[152] ONCIX REPORT, *supra* note 12, at 2–3, A-4.

[153] *See, e.g.*, STRATEGY REPORT, *supra* note 9, at 4–5; *see also* Kelley Clements Keller & Brian M.Z. Reece, *Economic Espionage and Theft of Trade Secrets: The Case for a Federal Cause of Action*, 16 TUL. J. TECH. & INTELL. PROP. 1, 4, 23–27 (2014) (suggesting that

Notably absent from the materials circulated by the United States is reference to the goal of promoting progress. Congress enacted the EEA under its Commerce Clause authority,[154] and it is clear that protecting America's edge in commerce is how it is being applied. Toren's analysis makes the point. He shows that as of 2012, of the 124 cases brought, 115 involved theft, not economic espionage intended to benefit foreign governments;[155] often, the cases that were targeted were ones where the defendant's goal was to launch a start-up.[156]

III. REPERCUSSIONS

The new rhetoric of trade secrecy has led to statutory changes in the EEA, looser interpretations of its provisions, and significantly increased prosecution. With more investigations and convictions, along with a new view of national security, there is also a new risk: that instead of protecting U.S. leadership in science and technology, these developments will alter the creative environment in ways that chill progress. This Part discusses these two issues.

A. Impact of the New Rhetoric on EEA Prosecutions

In his article on trade secrecy as an instrument of national security, Aaron Burstein argued that the EEA actually has perverse consequences for national security.[157] Because foreign militaries are not their rivals, private firms do not internalize all of the national security benefits that flow from keeping information out of the hands of enemy governments. Increasing deterrence—and knowing the FBI to be on call in case of intrusions—only makes matters worse because it gives firms even more reason to skimp on their own security measures.[158] Burstein suggested ramping up the EEA.[159] While he ultimately rejected the idea of making firms criminally liable for losing high tech information or for failing to report

---

the nexus with security requires supplementing government prosecution with private remedies).

[154] United States v. Agrawal, 726 F.3d 235, 248 (2d Cir. 2013) ("The EEA's nexus provision . . . signals Congress's intent to exercise its Commerce Clause authority to address the theft of trade secrets.").

[155] Toren, *supra* note 9.

[156] *Id.* (noting that "in approximately 70 percent of the cases in which the purpose of the theft was discoverable, the defendant committed the theft in order to help start a new company or for personal use").

[157] Burstein, *supra* note 38, at 947–48.

[158] *Id.* at 948, 979.

[159] *Id.* at 980.

breaches of security,[160] he did consider relaxing other elements of the crime.[161]

To a certain extent, that is exactly what has happened. The Attorney General's approval is no longer required for prosecutions for theft (it is for espionage).[162] Moreover, the critical restriction—that the trade secret be embodied in a product in commerce—disappeared in 2012 in response to the Second Circuit's decision to overturn Aleynikov's EEA conviction. Under the Theft of Trade Secrets Clarification Act,[163] it is not only secrets embedded in products that are actionable; secrets embedded in services (such as high-frequency trading services) are too.[164] More important, a prosecutor need only show that a product or service was "intended for use" in commerce, not that it actually entered commerce.[165] Therefore, mere knowledge of potential uses may be sufficient. For example, DOJ now considers this element met if the prosecution can show use in research that will lead to the development of a product or service.[166]

More generally, the Justice Department's current view of the scienter requirements leaves prosecutors with considerable scope. Relying on the legislative history, the DOJ now argues that the knowledge requirements can be satisfied with a showing that the defendant *should have known* the facts in issue; actual knowledge is not required.[167] In the DOJ's opinion, the prosecutor need not show the defendant knew that the sub-elements of what constitutes a trade secret were present (e.g., that reasonable measures were taken) or even that the information was a trade secret, so long as the defendant knew it was proprietary information.[168] Given the ONCIX Report's view of what constitutes a trade secret, that is not a very high barrier.[169] Indeed, in the employment context it is often not a barrier at all, because many employers, as a matter of routine, require employees to sign employment contracts that define almost any and all in-

---

[160] *Id.* at 981–82.

[161] *Id.* at 980–81.

[162] IP CRIMES MANUAL, *supra* note 11, at 184.

[163] 18 U.S.C. § 1832(a).

[164] *Id.*

[165] *Id.*

[166] IP CRIMES MANUAL, *supra* note 11, at 187–89 (noting also that the post-*Aleynikov* amendment relaxed the view on what constitutes commerce).

[167] *Id.* at 178.

[168] *Id.* at 178–79.

[169] *Id.* ("[A] defendant must know that the information he or she seeks to steal is proprietary, meaning belonging to someone else who has an exclusive right to it, but does not have to know that it meets the statutory definition of a trade secret." (citing United States v. Roberts, No. 3:08-CR-175, 2009 WL 5449224, at *5 (E.D. Tenn. Nov. 17, 2009))); *see also* DOYLE, *supra* note 15, at 5–6 (stressing that the EEEA should not be "unnecessarily narrowed").

formation learned on the job as proprietary.[170] While knowledge of committing a listed act is still required, these are so mundane that they too do not impose a significant hurdle.[171] And because the ONCIX Report and the Targeting Analysis consider even more activities "methods of economic espionage,"[172] this element may be watered down even further.

To prove espionage, the government is required to show intent to benefit a foreign government, but prosecutors interpret that broadly as well: The focus is on the defendant's subjective belief, not on whether an actual benefit accrues.[173] Moreover, "benefit" can include "reputational, strategic, or tactical benefit."[174] Nor must the foreign government own the entirety of the entity to be benefited. For theft, intent to confer an economic benefit is required, as is intent to injure the owner of the trade secret. However, in the government's view, circumstantial evidence can prove the latter, such as lying about post-employment plans.[175] Further, the emphasis is on intent, not actual benefit or injury. As the 2014 Congressional Overview states it: "[T]he element addresses the defendant's state of mind, not reality. Nothing in the statute's language demands that the government prove actual injury."[176] Indeed, because it is now recognized that even knowledge of blind alleys (knowing what not to try) is associated with savings,[177] DOJ could even relax the requirement that prosecutors concentrate on a specific piece of information.[178] Of course, courts may not agree with the DOJ's position on all these issues. Still, the threat of prosecution—and in some cases, the aftermath of prosecution[179]—may well deter socially important exchanges.

Nor is it likely that constitutional jurisprudence will continue to ensure that the Act is interpreted with sensitivity to access interests. In *Golan v. Holder*, [180] the Supreme Court held that Congress can remove material from the public domain if it reasonably believes the result will promote

---

[170] Lobel, *supra* note 30, at 810.

[171] Pooley et al., *supra* note 68, at 192–94.

[172] *See* ONCIX Report, *supra* note 12, at 2–3.

[173] IP CRIMES MANUAL, *supra* note 11, at 183.

[174] *Id.*

[175] *Id.* at 185–86.

[176] DOYLE, *supra* note 15, at 5.

[177] *Cf.* United States. v. Howley, 707 F.3d 575 (6th Cir. 2013) (noting problems in evaluating the harm for sentencing purposes). *See generally* Charles Tait Graves, *The Law of Negative Knowledge: A Critique*, 15 TEX. INTELL. PROP. L.J. 387 (2007).

[178] *See supra* text accompanying note 73.

[179] *See, e.g.*, Nicole Perlroth, *Chinese-American Cleared of Spying Charges Now Faces Firing*, N.Y. TIMES (Sept. 15, 2015), http://nyti.ms/1ifapFc (noting that even after Sherry Chen, a hydrologist at the National Weather Service, was cleared of charges under the EEA, the government decided to fire her.).

[180] Golan v. Holder, 132 S. Ct. 873, 886 (2012).

intellectual progress. And in *United States v. Martignon*,[181] the Second Circuit held that criminal statutes protecting intellectual creations (in that case, unfixed copyrightable works) are sufficiently different from the kinds of intellectual property law authorized by the Copyright and Patent Clause to avoid the problem of using the Commerce Clause to end-run limitations on Congressional authority.[182] The result is that, even if Toren was right in 2012 when he found that the government only went after more than "garden variety" theft, the future may well involve more troubling prosecutions.[183] The U.S. Attorneys' Manual, which stresses the deterrence value of prosecution, is suggestive:

> The availability of a civil remedy should not be the only factor considered in evaluating the merits of a referral because the victim of a trade secret theft almost always has recourse to a civil action. The universal application of this factor would thus defeat the Congressional intent in passing the EEA.[184]

The danger of escalating prosecution is borne out statistically. Since 2013, the Administration has begun to pursue more investigations and increase the number of indictments for economic espionage. Compared to the previous year, the number of prosecutions increased by over 30%, and in 2014, the number again increased by over 33%.[185] Over half of the economic espionage indictments since 2013 have had a China connection.[186] A look at a few of the cases demonstrates this trajectory. Hanjuan Jin, a naturalized American citizen of Chinese descent who obtained two graduate degrees from American universities, was convicted of misappropriating Motorola's iDEN technology and sentenced to 48 months in jail.[187] Jin was caught red-handed with thousands of Motorola documents while using a one-way ticket to fly to China, where she planned to work for a Chinese competitor of her former employer.[188] However, the information she had—"push-to-talk" capabilities—was known in the industry.[189] While iDEN was a complete end-to-end system that one witness testified had the fastest push-to-talk capability, the technology was arguably

---

[181] United States v. Martignon, 492 F.3d 140 (2d Cir. 2007).

[182] *Id.* at 145–52.

[183] Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172, 225 (2014).

[184] U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL § 9-59.100 (2015), http://www.justice.gov/usam/usam-9-59000-economic-espionage.

[185] Perlroth, *supra* note 10, at 2–3.

[186] *Id.* Between January 2009 and January 2013, China was involved in 17 criminal prosecutions (out of a total of 20) under the EEA. *See* STRATEGY REPORT, *supra* note 9, at annex 3.

[187] United States v. Hanjuan Jin, 733 F.3d 718, 719 (7th Cir. 2013).

[188] *Id.* at 720.

[189] *Id.*

already losing its commercial cachet.[190] Thus, Jin claimed she was taking the material with her as a study aid and to refresh her knowledge.[191] Nevertheless, the Seventh Circuit affirmed her conviction, reasoning:

> [W]hat she was studying—what she was refreshing her knowledge of—was iDEN. In China she would be a walking repository of knowledge about iDEN that she could communicate to any company or government agency interested in hacking or duplicating iDEN. Could and would, because it would enhance her career prospects; what other motive could she have had for refreshing her knowledge of iDEN? So had she not been stopped from boarding the plane to China, she would have succeeded in conferring an economic benefit on herself and [her future employer], and quite possibly on the Chinese military as well.
>
> The government doesn't have to prove that the owner of the secret actually lost money as a result of the theft. For remember that the "independent economic value" attributable to the information's remaining secret need only be "potential," as distinct from "actual."[192]

Similarly, Wen Chyu Liu, who worked for Dow Chemical Company from 1965 to 1992 and had security clearance, was convicted for taking technology he had helped create for use in a firm he started with his wife.[193] On appeal, Liu challenged the trial court's exclusion of an expert who would have testified that the material taken was generally known in the industry. Although under a standard trade secrecy analysis, that information would be crucial to the question of whether unlawful misappropriation occurred, the Fifth Circuit sustained the conviction, holding that, while the district court erred in excluding the expert, that error was harmless.[194]

Some of the prosecutions clearly go overboard in their intense focus on Chinese nationals. In a 2014 case, Sherry Chen, a National Weather Service hydrologist who specialized in forecasting flood threats, was met soon after a visit of her family in China by six FBI agents. Chen, born in China and a naturalized American citizen, was accused of using a stolen password to download information about the nation's dams and meeting with a high-ranking Chinese official.[195] She was told she faced 25 years in prison and $1 million in fines. The case was investigated for months—

---

[190] *Id.*

[191] *Id.* at 721.

[192] *Id.*

[193] United States v. Wen Chyu Liu, 716 F.3d 159, 161–62 (5th Cir. 2013), *cert. denied*, 134 S. Ct. 1011 (2014).

[194] *Id.* at 169.

[195] Perlroth, *supra* note 10.

right up until the FBI suddenly dropped it.[196] In an interview about the case, even Peter Toren expressed concern about where the government is going with this type of prosecution. As he put it: "They came across a person of Chinese descent and a little bit of evidence that they may have been trying to benefit the Chinese government, but it's clear there was a little bit of Red Scare and racism involved[.]"[197] Similarly, former Justice Department espionage and computer-crimes prosecutor Mark Rasch reviewed the Chen case and concluded that even though "[t]he government thought they had struck gold with this case . . . the facts didn't quite meet the law here. . . . If you're looking everywhere for spies, you will find spies everywhere, even where they don't exist[.]"[198]

In May 2015, following the media coverage of the Chen case, twenty-two members of Congress asked the Attorney General to determine whether race played a factor in the handling of federal investigations and questioned whether there was a growing practice of targeting federal employees based on their national origin.[199] In the letter, the representatives raise the concern that "[f]ederal employees are trained that naturalized citizens are more suspicious and that people who speak a foreign language at home are more suspicious."[200]

B. Impact of the New Rhetoric on the Creative Environment

For innovation, the real question is not how much the EEA criminalizes, but what criminalization under a broad view of promoting national security does to the pace of technological development. The national security view of trade secret protection is static—it is intended to safeguard the current position of the technology industry in the United States. In a sense, then, it offers strong protection for what is *already* known. But intellectual property law, upon which the EEA was based, was meant to have a dynamic effect—it was aimed at fostering *future* technological development. As discussed earlier, early EEA prosecutions tried to accommodate this goal and to a large extent, succeeded.[201] But the government's shift to a security frame makes it necessary to reconsider the statute's impact. Based on experience with similarly structured security safeguards, we fear that the ramifications for university-based research

---

[196] *Id.*

[197] *Id.* Even after charges were dropped, Chen was fired. *See supra* note 179.

[198] *Id.*

[199] Nicole Perlroth, *Members of Congress Ask for Review of Dropped Espionage Case*, N.Y. TIMES (May 21, 2015), http://bits.blogs.nytimes.com/2015/05/21/members-of-congress-ask-for-review-of-dropped-espionage-case/ (noting that Representative Ted Lieu, a Democrat of California, explained the concern as based on "a history of discrimination against Asian Pacific Americans, [where] the recurrent theme is one of suspicion").

[200] *Id.*

[201] *See supra* Part II.

and high tech employment could be considerable. Ultimately, the global community must ask whether a highly interlocking set of protections against trade secret leakage will pose a barrier to innovation and undermine social welfare.

1. University Research.

Many recent prosecutions under the EEA have involved university research. As noted earlier, the government appears particularly concerned about what goes on in the academy—it measures losses by reference to research grants; it considers conferences and publications a means for espionage; some of the cases have involved university researchers.[202] Under a view that equates national security with innovation preeminence, it is not surprising that this would be so. As Vannevar Bush, architect of U.S. science policy, put it, universities are the engine of innovation[203]: academia focuses on fundamental science, with important spillover benefits for industry, commerce, healthcare, and the military. Not only does the federal government invest heavily in this work,[204] it has also

---

[202] *See supra* notes 109–116 and accompanying text; *see also* Hearing Charter at 1, *Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation While Protecting Critical Information: Hearing Before the Subcomm. on Oversight of the H. Comm. on Sci., Space & Tech.*, 113th Cong. (2013) [hereinafter *Oversight Hearing Charter*], http://docs.house.gov/meetings/SY/SY21/20130516/100836/HHRG-113-SY21-20130516-SD002.pdf (measuring the value of stolen research by the cost of funding it); Josh Cornfield, *A Temple University Professor Faces 80 Years in Prison over Charges that He Passed Tech Secrets to China*, BUS. INSIDER (May 22, 2015), http://www.businessinsider.com/a-temple-university-professor-faces-80-years-in-jail-for-allegedly-planning-to-pass-tech-secrets-to-china-2015-5; Daniel Golden, *American Universities Infected by Foreign Spies Detected by the FBI*, BLOOMBERG BUS. (Apr. 8, 2012), http://www.bloomberg.com/news/articles/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi; Ellen Nakashima, *U.S. Indicts 6 Chinese Citizens on Charges of Stealing Trade Secrets*, WASH. POST (May 19, 2015), https://www.washingtonpost.com/world/national-security/us-indicts-6-chinese-on-charges-of-stealing-trade-secrets/2015/05/19/f11fd35e-fdd8-11e4-805c-c3f407e5a9e9_story.html (noting the indictment of students who had obtained engineering degrees at the University of Southern California and then secured jobs at high tech firms in China, taking with them information intended to benefit Tianjin University, a state school); Bruce Veilmetti, *Medical College of Wisconsin Researcher Charged with Economic Espionage*, MILWAUKEE-WISC. J. SENTINEL (Apr. 1, 2013), http://www.jsonline.com/news/crime/medical-college-researcher-charged-with-stealing-anticancer-compound-ls9cnn4-200958961.html.

[203] VANNEVAR BUSH, SCIENCE: THE ENDLESS FRONTIER 15 (1945).

[204] RONDA BRITT, NAT'L SCI. FOUND., UNIVERSITIES REPORT $55 BILLION IN SCIENCE AND ENGINEERING R&D SPENDING FOR FY 2009; REDESIGNED SURVEY TO LAUNCH IN 2010 (Sept. 2010), http://www.nsf.gov/statistics/infbrief/nsf10329/nsf10329.pdf; Joshua A. Newberg & Richard L. Dunn, *Keeping Secrets in the Campus Lab: Law, Values and Rules of Engagement for Industry–University R&D Partnerships*, 39 AM. BUS. L.J. 187, 193 (2002) (noting that the federal government historically funds around 60–70% of academic research). According to the Association of American Universities, in 2009, the federal government supported about $33 billion of universities' total annual R&D spending

turned universities into what Liza Vertinsky calls the "guardians of invention,"[205] charged with the task of translating the science into technology and stewarding it to commercial application. Through initiatives like the Bayh–Dole Act,[206] which allows universities to hold patent rights in federally funded research, academia has become a custodian of intellectual property rights and its efforts are often measured in terms of the patents and associated know-how that they generate and license out.[207] Universities now spin off start-up companies, enter into research joint ventures with private industry, and permit (indeed, encourage) their faculty members to play major roles in private research and development entities.[208] The sum total of these activities makes universities appear to be the equivalent of private industry and the information they generate an appropriate subject for trade secret protection under civil and criminal law. Or to put it another way, if the new goal of trade secret law is to protect the United States' dominant position in technology, it is easy to perceive the university as a key place to police behavior.

But this view of universities misses much that is important about how it is that they play this remarkable role. To address challenging and complex problems, researchers must work collaboratively with those in other disciplines and from other backgrounds. To succeed, faculty must be perceived as good collaborators and mentors; they must publish and present their work at conferences, visit with others in their field, and provide space to visitors from other universities and industry.[209] Increasingly, it is

---

of $55 billion. *See* ASS'N OF AM. UNIVS., UNIVERSITY RESEARCH: THE ROLE OF FEDERAL FUNDING (Jan. 2011), https://www.aau.edu/WorkArea/DownloadAsset.aspx?id=11588. According to an NSF report, the federal government provided $38.9 billion (63%) of the $62.3 billion of academic spending on science and engineering R&D in FY 2012. NAT'L SCI. BD., SCIENCE AND ENGINEERING INDICATORS 2014 ch. 5 (2014), http://www.nsf.gov/statistics/seind14/content/chapter-5/chapter-5.pdf.

[205] *See generally*, Liza Vertinsky, *Universities as Guardians of Their Inventions*, 2012 UTAH L. REV. 1949.

[206] University and Small Business Patent Procedures Act of 1980, 35 U.S.C. §§ 201–211 (2012). *See generally* Rochelle Cooper Dreyfuss, *Double or Nothing: Technology Transfer Under the Bayh–Dole Act*, *in* BUSINESS INNOVATION AND THE LAW: PERSPECTIVES FROM INTELLECTUAL PROPERTY, LABOUR, COMPETITION AND CORPORATE LAW 52, 54–56 (Marilyn Pittard, Ann L. Monotti & John Duns eds., 2013).

[207] *See, e.g.*, *AUTM Licensing Activity Survey: FY2014*, ASS'N U. TECH. MANAGERS, http://www.autm.net/resources-surveys/research-reports-databases/licensing-surveys/fy-2014-licensing-survey/; NAT'L RESEARCH COUNCIL, MANAGING UNIVERSITY INTELLECTUAL PROPERTY IN THE PUBLIC INTEREST 3, 19 (2011).

[208] *See, e.g.*, Jason Owen-Smith & Walter W. Powell, *The Expanding Role of University Patenting in the Life Sciences: Assessing the Importance of Experience and Conductivity*, 32 RES. POL'Y 1695, 1695–1711 (2003); *see also* Newberg & Dunn, *supra* note 204, at 196–97.

[209] *See* Walter M. Powell, *Networks of Learning in Biotechnology: Opportunities and Constraints Associated with Relational Contracting in a Knowledge-Intensive Field*, *in*

crucial that travel and collaboration occur internationally. Because students and post-doctoral fellows perform much of the day-to-day research—and because education is also a public goal of universities—universities work hard to create an attractive environment conducive to learning and to research.

To be sure, the incentives that propel researchers are partly monetary, and are thus compatible with trade secrecy. However, the classic rewards of academia are satisfying curiosity,[210] solving the puzzle of how the world works, enjoying the intrinsic satisfaction of research and discovery,[211] and obtaining public recognition.[212] To accomplish these objectives, governance by Mertonian norms is critical, especially the norm of communitarianism—the conviction that work must be communicated and shared so that others can verify it (through peer review), build upon it, and determine priority of invention.[213] University-generated information is thus situated in a complex domain. It is not exactly public, since it can be subject to contractual obligations and intellectual property rights. But it is not private either. Michael Madison, Brett Frischmann, and Katherine Strandburg call it an information "commons": universities are internally and jointly organized to pool knowledge resources, even when externally structured to, in some instances, require payment from others.[214]

Even within universities, the complexity of this terrain is problematic, for proprietary goals can conflict with the university's broader mission

---

EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY 251, 254–55 (Rochelle Cooper Dreyfuss, Diane Leenheer Zimmerman & Harry First eds., 2001); Walter W. Powell, *Inter-Organizational Collaboration in the Biotechnology Industry*, 152 J. INSTITUTIONAL & THEORETICAL ECON. 197, 205 (1996).

[210] *See, e.g.*, Brian J. Love, *Do University Patents Pay Off? Evidence from a Survey of University Inventors in Computer Science and Electrical Engineering*, 16 YALE J.L. & TECH. 285, 316 (2014) (showing that the major motivating factor for university computer scientists is curiosity and a desire to advance knowledge).

[211] *See generally* Alice Lam, *What Motivates Academic Scientists to Engage in Research Commercialization: 'Gold', 'Ribbon' or 'Puzzle,'* 40 RESEARCH POL. 1354 (2011).

[212] The latter includes prizes, naming rights for new discoveries, extra laboratory space—some of which can be cashed out in the form of prizes and promotion. *See* Rebecca S. Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L.J. 177, 181–84 (1987); Rebecca S. Eisenberg, *Public Research and Private Development: Patents and Technology Transfer in Government-Sponsored Research*, 82 VA. L. REV. 1663, 1700 (1996); Katherine J. Strandburg, *Curiosity-Driven Research and University Technology Transfer*, *in* UNIVERSITY ENTREPRENEURSHIP AND TECHNOLOGY TRANSFER: PROCESS, DESIGN, AND INTELLECTUAL PROPERTY 93, 94–95 (Gary D. Libecap ed., 2005).

[213] *See* ROBERT K. MERTON, THE SOCIOLOGY OF SCIENCE: THEORETICAL AND EMPIRICAL INVESTIGATIONS 273–74 (1973).

[214] Michael J. Madison, Brett M. Frischmann & Katherine J. Strandburg, *The University as Constructed Cultural Commons*, 30 WASH. U. J.L. & POL'Y 365 (2009).

to discover, educate, and spread knowledge. To combat the perception that patents and licenses are the sole measure of their scientific contributions, MIT conducted a comprehensive study of its activities, which demonstrated the outsize role that free technology transfer plays in keeping the nation at the technological frontier.[215] The University of California at Berkeley has pioneered methods of evaluating technology transfer offices that take account of non-proprietary transfers.[216] Although universities enter into many ventures with private firms, they routinely guard against agreements that prohibit publication, require significant delays, or jeopardize the ability of their faculty or students to share information.[217] The Association of University Technology Managers (AUTM), for example, has promulgated a list of points to consider in university licensing that has been signed by many major universities and medical colleges.[218] The points include making sure that licensing agreements do not restrict university faculty from engaging in future research, structuring licenses to encourage technology development, ensuring broad access to research tools, and—significantly—taking a cautious approach to enforcing intellectual property rights.[219]

Universities have been particularly alert to successive attempts by the government to interfere with this complex ecology in the name of national security.[220] In the 1980's, amid concerns about the Soviet Union, Admiral Bobby Inman, at one time Deputy Director of the CIA, gave a speech at the American Association for the Advancement of Science raising many of the same themes we see today:

> [F]oreign intelligence services . . . are collecting all types of information in the U.S. Specific data on technical subjects are high on the wanted list of every major foreign intelligence service and for good reasons . . . . In terms of harm to the national interests, it makes little difference whether the data are copied from technical

---

[215] Edward B. Roberts & Charles Eesley, Mass. Inst. of Tech., Entrepreneurial Impact: The Role of MIT (2011), https://ilp.mit.edu/media/webpublications/pub/literature/Entrepreneurial-Impact-2011.pdf.

[216] Carol Mimura, *Nuanced Management of IP Rights: Shaping Industry–University Relationships to Promote Social Impact*, *in* Working Within the Boundaries of Intellectual Property: Innovation Policy for the Knowledge Society 269 (Rochelle C. Dreyfuss, Harry First & Diane L. Zimmerman eds., 2010).

[217] *See* Newberg & Dunn, *supra* note 204, at 209–10. *See generally* Rebecca S. Eisenberg, *Academic Freedom and Academic Values in Sponsored Research*, 66 Tex. L. Rev. 1363 (1988).

[218] Ass'n of Univ. Tech. Managers, In the Public Interest: Nine Points to Consider in Licensing University Technology (2007) [hereinafter Nine Points], http://www.autm.net/AUTMMain/media/Advocacy/Documents/Points_to_Consider.pdf.

[219] *Id.* at points 1, 2, 5, 6.

[220] *See* Eisenberg, *supra* note 217, at 1375.

> journals in a library or given away by a member of our society to an agent of a foreign power . . . .[221]

To stop the "hemorrhag[ing],"[222] Inman proposed that the government exert greater control over the release of technological information.[223] But to a large extent, universities successfully resisted his proposal.[224] In 1985, President Reagan promulgated NSDD-189, a national policy on technology transfer that protects fundamental research by exempting unclassified information from various forms of control.[225] Although the policy statement warned about the acquisition of information by Eastern Bloc Nations and acknowledged that some research may be classified, it also recognized that American leadership required an "environment in which the free exchange of ideas is a vital component"[226] and firmly stated that to the "maximum extent possible, the products of fundamental research remain unrestricted."[227] After the attack on the World Trade Center in September 2001, much the same thing happened. Concerns over information transfer were expressed, but the Bush administration ultimately confirmed that NSDD-189 remained in effect.[228] Even so, many universities have been concerned. The National Academies of Science has issued a series of recommendations to ensure the NSDD-189 policy is continued.[229]

Universities have also directly monitored the manner in which export control laws and visas are administered.[230] These laws have been subject to varying interpretations, leading to attempts to exert extraordinary levels of control over the distribution of fairly common laboratory tools, and to consider the act of sharing even certain unclassified information with foreigners (even those with green cards) as a deemed export, sub-

---

[221] Bobby R. Inman, Striking a Balance: Scientific Freedom and National Security, at the Annual Meeting of the AAAS, Washington, D.C. (Jan. 7, 1982) (quoted in Edward Gerjuoy, *Controls on Scientific Information Exports*, 3 YALE L. & POL'Y REV. 447, 459 (1985)).

[222] *Id.* at 460.

[223] *Id.* at 459.

[224] Rosemary Chalk, *Security and Scientific Communication*, BULL. ATOMIC SCIENTISTS, Aug.–Sept. 1983, at 19.

[225] National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical and Engineering Information (Sept. 21, 1985), https://research.archives.gov/id/6879779.

[226] *Id.*

[227] *Id.*

[228] NAT'L RESEARCH COUNCIL, SCIENCE AND SECURITY IN A POST 9/11 WORLD: A REPORT BASED ON REGIONAL DISCUSSIONS BETWEEN THE SCIENCE AND SECURITY COMMUNITIES 30 (2007), http://www.ncbi.nlm.nih.gov/books/NBK11495/.

[229] *See id.* at 7–33.

[230] For a summary of export control laws, see generally IAN F. FERGUSSON & PAUL K. KERR, CONG. RESEARCH SERV., R41916, THE U.S. EXPORT CONTROL SYSTEM AND THE PRESIDENT'S REFORM INITIATIVE (2014), https://www.fas.org/sgp/crs/natsec/R41916.pdf.

ject to regulation.[231] Although actions in 2005 and 2006 brought some clarity to both export and deemed-export regulations,[232] and in 2009, President Obama launched a comprehensive review aimed at creating a single unified system of export review,[233] the laws remain a topic of National Academies recommendations and AUTM concern.[234] Analogous problems have occurred with visas. After 9/11, the government increased the time necessary to process visas, affecting not only the job market but also universities and graduate students.[235] Such problems ended when universities complained about interference with scientific collaborations, the flow of scientific talent, and the timing of important conferences.[236]

In light of the success universities have had at protecting their information commons, one might think they would be equally able to thwart heavy-handed applications of the EEA. But in many ways, the EEA presents a much more pernicious problem than classification systems, export and deemed-export controls, and visas because it covers more activities. Moreover, universities are not as well positioned to deal with its impact. First, the government has long recognized that direct controls over information transfers implicate important scientific and academic values. NSDD-189 states as much and—with regard to exports, deemed exports, and visas—the government undertakes to maintain consistency

---

[231] *Id.* at 1, 13.

[232] *See* Benjamin Carter Findley, Comment, *Revisions to the United States Deemed-Export Regulations: Implications for Universities, University Research, and Foreign Faculty, Staff, and Students*, 2006 WIS. L. REV. 1223, 1228–31; *see also* William Metcalf, *Do Higher Education Institutions Have a Misunderstanding of the Fundamental Research Exemption: How Export Control Regulations Change University Research*, 39 J.L. & EDUC. 281 (2010).

[233] *See* FERGUSSON & KERR, *supra* note 230, at 10–15.

[234] *See* NAT'L RESEARCH COUNCIL, *supra* note 228, at 40–47; *see also* NAT'L RESEARCH COUNCIL, BEYOND 'FORTRESS AMERICA': NATIONAL SECURITY CONTROLS ON SCIENCE AND TECHNOLOGY IN A GLOBALIZED WORLD (2009), http://www.nap.edu/catalog/12567/beyond-fortress-america-national-security-controls-on-science-and-technology; NINE POINTS, *supra* note 218, at point 7.

[235] Michael A. Olivas, *IIRIRA, the DREAM Act, and Undocumented College Student Residency*, 30 J.C. & U.L. 435, 457–63 (2004).

[236] Yudhijit Bhattacharjee, *U.S. Promises to Reduce Delays in Granting Visas for Scientists*, 324 SCIENCE 1377 (2009) (noting especially delays for applicants from China); *see also* NAT'L RESEARCH COUNCIL, *supra* note 234, at 11 ("The United States cannot protect U.S. jobs by denying entry to foreign professionals; jobs will simply go abroad. It is important for both the national security and economic prosperity to maintain the flow of human talent into the United States."). Stanford University reportedly avoids seeking contracts for export-controlled research, on which only Americans can work. University president John Hennessy stated at a 2010 congressional hearing in Palo Alto that "Stanford does not, nor will it, restrict participation of students on the basis of citizenship." Golden, *supra* note 202.

with this reality.[237] No similar effort has been made regarding the EEA. Second, one aspect of the accommodation is a complex classification system that focuses on the potential military applications of particular technologies.[238] A frame that equates technological dominance with national security puts the focus on the status of the information as proprietary, regardless of its potential application. Third, regulations are adopted centrally, by individual agencies or under President Obama's new initiative, by a consortium of regulators. EEA prosecutions are largely decentralized and, for theft, left to the discretion of individual prosecutors, which means there may be little consideration given to the cumulative impact of these efforts on the university community.

Most important, export, deemed-export, and visa regulations directly affect universities and university administrators. Accordingly, slippages in the definition of sensitive information or the activities labeled as suspect quickly come to their attention. As we saw, the National Academies, which has a longstanding interest in the problem, acts as a strong advocate for university interests in open science, yet it has not commented on the effect of the EEA.[239] The reason may be that university administrators have little occasion to review documents like the Department of Justice's IP Crimes Manual. And because prosecutions generally involve transfers of information to foreign universities, administrators do not see indictments either. Indeed, because their involvement is framed as the victims of crime, there is little occasion for universities to systematically consider how the EEA affects their roles as centers of fundamental research.

In addition, the FBI seems intent on developing a cozy relationship with the academy and appears to a large extent to be successful in these efforts.[240] A recent news article, titled *American Universities Infected by Foreign Spies Detected by FBI*, describes instances of universities, consulting with the FBI, refusing funds and students because of the fear they might come with hidden foreign agendas to steal information.[241] The article describes a professor at University of Colorado who decided to stop accepting visiting scholars from China because one such student asked questions that "made him uncomfortable."[242] The piece also quotes FBI offi-

---

[237] *See, e.g.*, *Oversight Hearing Charter*, *supra* note 202, at 2; Memorandum on Fundamental Research from Ashton B. Carter, Under Sec'y of Def., to Sec'ys of the Military Dep'ts 1–2 (May 24, 2010), http://fas.org/irp/doddir/dod/research.pdf.

[238] *See Oversight Hearing Charter*, *supra* note 202, at 6 ("Classification is the most appropriate mechanism when it is required that certain information be maintained in confidence in order to protect American citizens and national security.").

[239] *See* NAT'L RESEARCH COUNCIL, *supra* note 228.

[240] Golden, *supra* note 202 (quoting the statement of Frank Figliuzzi, FBI assistant director for counterintelligence that "[t]he FBI and academia, which have often been at loggerheads, are working together to combat the threat").

[241] *Id.*

[242] *Id.*

officials warning against attempts to steal trade secrets from universities through "academic solicitation,"[243] including "requests to review academic papers or study with professors."[244] It notes that invitations to present papers at international conferences or to visits research labs can be a set up for predatory espionage, and it suggests that foreign exchange programs are a prime target for stealing valuable knowledge.[245]

Nor are universities in a position to complain about how the statute is interpreted in individual cases. Prosecutions are not targeted at a university, but rather at individual faculty members—indeed, at individuals who *left* the university, often to work at a global rival.[246] The university is thus in the posture of a victim and may not have an interest in helping such defendants. Even if it did, the university would have no formal role in the criminal trial or appeal and thus would lack opportunity to present arguments about whether the information taken should be considered a trade secret, whether the defendant's activities should be thought to constitute misappropriation, or whether the value of the information was such that the defendant could have rationally formulated the intent to benefit a foreign government (for espionage) or injure the owner of the information (for theft).[247]

Because EEA prosecutions are more episodic than export controls, it could be argued that their effect is less deleterious. But that seems unlikely. The goal of criminal law is deterrence and if prosecutions are stepped up as planned, the EEA could be very effective. Academics may not be completely judgment proof, but they are probably relatively insensitive to the prospect of civil liability for trade secret violations. They are, however, likely to be very concerned by the prospect of incarceration. To compound the problem, ownership of collaborative projects can be murky in academic settings.[248] There are few civil cases because faculty and students have reputational interests in not being viewed as litigious, but the cases that have become public demonstrate the difficulty of de-

---

[243] *Id.*

[244] *Id.*

[245] *Id.* ("'Study-abroad programs are an attractive target. Foreign security services find young, bright U.S. kids in science or politics, it's worth winning them over,' Figliuzzi said.").

[246] Andrew Grossman, *U.S. Charges Six Chinese Citizens with Economic Espionage*, WALL ST. J. (May 19, 2015), http://www.wsj.com/articles/u-s-charges-six-chinese-citizens-with-economic-espinoage-1432046527.

[247] These have proved to be challenging issues to which prosecutors do not always pay sufficient attention. *See, e.g.*, Matt Apuzzo, *U.S. Drops Charges that Professor Shared Technology with China*, N.Y. TIMES (Sept. 11, 2015), http://nyti.ms/1i4JCvk (describing a case that fell apart because the incriminating evidence turned out not to be a trade secret).

[248] For an example, consider Oliver Sacks' account of his clash with the director of the headache clinic at which he worked over the material in Sacks' book on migraines. *See* OLIVER SACKS, ON THE MOVE: A LIFE 150–58 (2015).

termining who has rights to slides, unique reagents, genetically altered specimens, and the like.[249] When raised in an EEA prosecution, these decisions could have life-altering consequences.[250]

The EEA could, in short, make American universities unattractive to students, post docs, visiting faculty, and other potential foreign collaborators. The recent arrests of three faculty members of China's Tianjin University highlights these risks. In the Chinese media reports of their arrests, Tianjin University officials stated that "the United States had done harm to academic exchanges by 'politicizing' a scientific dispute."[251]

There could also be unfortunate selection effects. Under a view of national security that seeks to preserve U.S. dominance, visitors from emerging countries, such as China and Russia, are likely to be the primary focus of investigations. But because these economies are so dynamic, these are the people with whom U.S. academics are probably most interested in collaborating. Furthermore, the premier universities in many countries are government-supported. Because exclusive ownership by the government is not necessary to consider an entity a foreign government, prosecution in these cases could be for economic espionage rather than theft.[252] Leading foreign faculty could, therefore, face especially stiff penalties. The National Academies has been concerned that export controls will hobble world-class scientists from coming to the United States, drive knowledge-intensive jobs abroad, and accelerate the development of foreign research centers;[253] paradoxically, the same can easily be said of an EEA administered with the goal of protecting U.S. technological leadership as a national security interest.

2. Job Mobility, Entrepreneurship, and Innovation

Most of the current charges under the Economic Espionage Act involve the scenario captured in *The Company Man*, where an employee—a

---

[249] *See* Rochelle Cooper Dreyfuss, *Collaborative Research: Conflicts of Authorship, Ownership, and Accountability*, 53 VAND. L. REV. 1161, 1165 (2000).

[250] *Cf.* Ann S. Jennings & Suzanne E. Tomkies, *An Overlooked Site of Trade Secret and Other Intellectual Property Leaks: Academia*, 8 TEX. INTELL. PROP. L.J. 241, 263–64 (2000) (suggesting attorneys and employees keep elaborate records).

[251] Michael Martina & Megha Rajagopalan, *China University Denies U.S. Economic Espionage Charges*, REUTERS (May 21, 2015), http://www.reuters.com/article/2015/05/21/us-usa-china-theft-idUSKBN0O60CU20150521. The article further reports calls by the Chinese media on the Chinese government "to respond more strongly to the case, calling the United States paranoid." *Id.* The Global Times, a nationalist tabloid, said, "The crime of espionage is the charge most abused by America." *Id.*

[252] *See* IP CRIMES MANUAL, *supra* note 11, at 182–84; *see also* David E. Sanger & Nicole Perlroth, *6 Chinese Men Indicted in Theft of Code from U.S. Tech Companies*, N.Y. TIMES (May 19, 2015), http://nyti.ms/1L6HCLs (describing the indictment of a Chinese Professor at Tianjin University, which is state-sponsored, on charges of economic espionage under § 1831).

[253] NAT'L RESEARCH COUNCIL, *supra* note 234, at 13.

lowly engineer, strapped for money and unable to send his child to the Ivy League college, is considered the weak link in the private company.[254] When this prototypical American worker is approached by a headhunter who offers him more for his talent, he naively considers it instead of immediately realizing that it must be a scam. When he finally "does the right thing" and goes to his boss to report on such preying, he is not offered a raise or promotion to match the (fake) outside offer. Rather, he is rewarded with the pat on the back for not falling for the predatory offer and is asked to cooperate with the FBI in a sting operation (perhaps for comedic effect, or perhaps to convey how difficult it is for a "civilian" to do the right thing, the film shows the FBI agents watching the engineer from the nearby hotel room during the sting operation and mocking him amongst themselves for almost getting sick from the fear of having to pose as a mole in order to capture the Chinese). The movie's dramatic climax centers on the ability of the frail employee to stay strong until the FBI bursts into the room to arrest the foreign offenders.

But not all employees are heroes and many find themselves on the receiving end of trade secret litigation. In civil cases involving trade secrets law in state courts the vast majority of the cases (over 90%) involve either a current or former employee or a business partner.[255] A similar pattern is emerging in criminal prosecutions involving the EEA. According to Toren's analysis, "[i]n more than 90 percent of the EEA prosecutions, the defendant was an 'insider,' and had access to the trade secret because he was an employee of the victim, or worked for a vendor or contractor of the victim." [256] In many of the cases the defendant committed the theft shortly before leaving the victim company.[257] In a 2000 Congressional hearing of the Subcommittee on International Economic Policy and Trade about enhancing laws against economic espionage, the chairman of the subcommittee's opening statement explained the threat posed by employees:

> [I]ndustrial espionage is a crime which continues to be best accomplished through low tech means and is not necessarily dependent upon high tech gadgetry.
>
> A vast majority of corporate espionage crimes do not occur in cyberspace, but rather in person, face to face. For example, key employees within a given corporation might be sought by a rival com-

[254] *The Company Man*, *supra* note 1; *see also* Rocket Media, *Betrayed*, VIMEO, https://vimeo.com/64908123 (second film made for the FBI).

[255] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZAGA L. REV. 57, 69 (2010).

[256] Toren, *supra* note 9.

[257] *Id.*

pany for information or recruited by spies posing as consultants or headhunters at trade shows.[258]

In general, intellectual property shapes competition and the flow of knowledge and people within industries and regions. Trade secrets in particular, because of their pervasiveness and their self-defining quality as encompassing whatever the company keeps confidential, affect the movement and behavior of employees. Therefore, while trade secret law is understood as a branch of intellectual property law, designed to draw boundaries around valuable proprietary information,[259] it should equally be understood as a system that regulates the relationship between firms and employees.[260] Quite straightforwardly, it is easy to see why increased trade secret protection operates to decrease employee mobility. In a legal regime of heightened trade secret liability, employees have more to lose when they choose to leave an employer. Prospective employers too are more at risk in such a regime. Beyond this direct effect on job recruitment, the key question for policy is how such a regime impacts innovation.

An impressive body of recent economic research considers the costs and benefits of job mobility, entrepreneurship, and knowledge flows for industries and regions. Overwhelmingly, the research on innovation shows the invaluable role of connectivity, knowledge networks, and exchanges for a region's economic health and innovation capacities.[261] Recent empirical studies in innovation consistently find that mobility and flow are correlated with higher levels of entrepreneurship and economic growth.[262] When individuals are allowed to move within an industry, they are able to deploy their skills and experience more effectively, and they are more motivated to perform well and grow professionally. Thus, recent behavioral research suggests that employees who are stripped of ownership over the knowledge and skills they gain during employment

---

[258] *Industrial Espionage Hearing*, *supra* note 87, at 2 (statement of chairperson Ileana Ros-Lehtinen).

[259] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 314 (2008).

[260] Lobel, *supra* note 30, at 811–12; Madhavi Sunder, *Trade Secret and Human Freedom*, *in* INTELLECTUAL PROPERTY AND THE COMMON LAW 334, 341–42 (Shyamkrishna Balganesh ed., 2013).

[261] *See, e.g.*, Jeffrey L. Furman & Scott Stern, *Climbing atop the Shoulders of Giants: The Impact of Institutions on Cumulative Research*, 101 AM. ECON. REV. 1933 (2011); Anders Malmberg & Dominic Power, *(How) Do (Firms in) Clusters Create Knowledge?*, 12 INDUS. & INNOVATION 409, 410 (2005).

[262] Matt Marx, Deborah Strumsky & Lee Fleming, *Mobility, Skills, and the Michigan Non-Compete Experiment*, 55 MGMT. SCI. 875 (2009); Sarah J. Taylor, Comment, *Fostering Economic Growth in the High-Technology Field: Washington Should Abandon Its Recognition of the Inevitable Disclosure Doctrine*, 30 SEATTLE U. L. REV. 473, 488–89 (2007).

are discouraged from investing in their human capital.[263] Again, this effect is not hard to comprehend: when employees understand that the knowledge and skill that they gain at a workplace is entirely proprietary and blocked from future use during the span of their career, they are less likely to be invested in gaining and building upon that knowledge.

Mobility has other important effects on technological progress. In mobile markets, knowledge networks are denser and the benefits of spillovers are spread not only to the receiving companies, but—counterintuitively—also to the "sending" companies, those who lose their employees to the competition.[264] The latter happens in several related ways. First, the company whose former employee moves to a related firm in the industry expands its company footprint by having denser connections, and a web of former employees in professional associations, technical committees, and lobbying efforts. This makes it easier for the "sending firm" to navigate the market. Second, firms are increasingly using their "alums" in similar ways as universities draw on their alumni: for recruitment purposes.[265] When potential hires know someone who used to work at a given company they are more likely to apply and to be interested in an opening at the firm. Former employees can be key goodwill ambassadors who enhance the firm's reputation.

Third and perhaps most important for innovation, when employees move from one company to another, both firms gain knowledge from these flows. In one study, a team of researchers from the Wharton School of the University of Pennsylvania and the University of Maryland studied the effects of "outbound mobility" on citation patterns in patent applications.[266] The study examined 154 semiconductor firms over 15 years and the linkages between the firms on both sides of an employee move. The study found that after an employee changed jobs, both the "sending" and the "receiving" firms become more likely to cite the other firm's pa-

---

[263] On Amir & Orly Lobel, *How Noncompetes Stifle Performance*, HARV. BUS. REV., Jan.–Feb. 2014, at 26; On Amir & Orly Lobel, *Driving Performance: A Growth Theory of Noncompete Law*, 16 STAN. TECH. L. REV. 833, 846 (2013); Lobel, *supra* note 30, at 848 ("In blunt economic terms, the deadweight loss from controls and restrictions over human capital is the person herself who is prevented from using her talent, skill, and passion. Minds are made to suppress ideas, skill remains untapped, knowledge is cut up into small fragments, and people risk their very liberty to move through their careers.").

[264] David B. Audretsch & Maryann P. Feldman, *R&D Spillovers and the Geography of Innovation and Production*, 86 AM. ECON. L. REV. 630 (1996); Tomas Havranek & Zuzana Irsova, *Estimating Vertical Spillovers from FDI: Why Results Vary and What the True Effect Is*, 85 J. INT'L ECON. 234 (2011).

[265] Orly Lobel, *Turnover Alchemy: Converting Employee Losses into Gains*, STRATEGY & BUS., Summer 2014, at 17.

[266] Rafael A. Corredoira & Lori Rosenkopf, *Should Auld Acquaintance Be Forgot? The Reverse Transfer of Knowledge Through Mobility Ties*, 31 STRATEGIC MGMT. J. 159 (2010).

tents.[267] That is, even companies that *lost* employees gained knowledge and access to the receiving firm's endeavors. The researchers suggest that the employees who remain in the sending firm benefit from information generated at their former colleague's new workplace by continued professional contact and through increased attention and awareness to the innovation activities of the receiving company, leading to cross-pollination.[268] The effect was more pronounced when there was a large geographic distance between the two companies.[269] This suggests that the farther an employee moves, for example, if a foreign-born employee returns to a home country to work at a rival firm there, the more significantly his or her former employer can benefit. The transfer creates a bridge between the firms and allows the employees of both firms to encounter intellectual capital that, as a practical matter, may otherwise have been unavailable to them.

Indeed, in sharp contrast to the traditional economic model, which posits that the more a firm is able to prevent exposure of their information, the more it will invest in research, recent empirical findings suggest that companies increase their investment in research and development when turnover is higher.[270] In this view, the research outputs of competing firms should, at least in some industries, be characterized as complementarities. Because innovation is cumulative in its nature, as knowledge flows throughout the industry, the entire industry, including those firms which experience the negative externalities of losing valuable knowledge to other firms in the field, moves more rapidly and increases its research outputs.[271] Building on these insights, the study of knowledge spillovers rejects a simplistic free-rider analysis and suggests that spillovers are increasing the equilibrium of R&D investment.[272] Industry, as well as

---

[267] *Id.* at 176.

[268] *Id.* at 177.

[269] *Id.* at 176.

[270] Paul Almeida & Bruce Kogut, *Localization of Knowledge and the Mobility of Engineers in Regional Networks*, 45 MGMT. SCI. 905, 915 (1999); Mark J. Garmaise, *Ties that Truly Bind: Noncompetition Agreements, Executive Compensation, and Firm Investment*, 27 J.L. ECON. & ORG. 376 (2011); Georg von Graevenitz, *Spillovers Reconsidered: Analysing Economic Welfare Under Complementarities in R&D* (Governance and the Efficiency of Econ. Sys., Discussion Paper No. 29, 2004), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=625142; Jiang He & M. Hosein Fallah, *Mobility of Innovators and Prosperity of Geographical Technology Clusters: A Longitudinal Examination of Innovator Networks in Telecommunications Industry* (Int'l Conference on Complex Sys., June 24–30, 2006).

[271] Tor Jakob Klette, Jarle Møen & Zvi Griliches, *Do Subsidies to Commercial R&D Reduce Market Failures?: Microeconometric Evaluation Studies*, 29 RES. POL'Y 471 (2000).

[272] Philippe Aghion & Xavier Jaravel, *Knowledge Spillovers, Innovation and Growth*, 125 ECON. J. 533 (2015).

regional, growth is endogenous; rather than a simplified win/lose dynamic, competition propels an upward cycle.[273]

Importantly, regions that encourage human capital mobility are also able to attract more human capital from other regions.[274] Conversely, regions that are too controlling of their human-capital flow experience over time a brain-drain effect, a movement away from the region by some of its most valuable talent.[275] Studies have documented the significance of foreign talent to the building of high tech regions, primarily Silicon Valley.[276] Historically, studies of innovation have consistently shown that traveling and foreign-born inventors are significantly over-represented among the great inventors.[277] Most broadly, the research suggests that high employee turnover, regional human-capital concentration, and density of professional networks all contribute to economic growth.[278] Putting the research on individuals and firms together, the interrelated effects suggest that at some point, too many constraints on the flow of knowledge and penalties on its use, especially when criminal sanctions are involved, can significantly reduce incentives to innovate.

The intensity of EEA prosecutions is particularly problematic from the viewpoint of job mobility and market competition. Even when the stakes merely involve civil trade secret litigation, disputes with former employers can have grave consequences. Litigation in these contexts is often used as a strategy to deter competition. As Graves and DiBoise note, "courts do not recognize that plaintiff's trade secret claims are too often created after the fact by attorneys to try to trap a former employee, and not so valuable that the plaintiff had previously recorded them as company intellectual property and guarded them as secret before the employee departed."[279] In other words, broad trade secret protections can have lock-in effects on workers. Employees are more likely to avoid jobs

---

[273] Paul M. Romer, *Endogenous Technological Change*, 98 J. POL. ECON. S71 (1990); Paul M. Romer, *The Origins of Endogenous Economic Growth*, 8 J. ECON. PERSP. 3 (1994).

[274] Charles I. Jones, *Human Capital, Ideas and Economic Growth*, *in* FINANCE, RESEARCH, EDUCATION AND GROWTH 51 (Luigi Paganetto & Edmund S. Phelps eds., 2003).

[275] Marx et al., *supra* note 262.

[276] ANNALEE SAXENIAN, THE NEW ARGONAUTS: REGIONAL ADVANTAGE IN A GLOBAL ECONOMY 50–52 (2006).

[277] B. Zorina Khan & Kenneth L. Sokoloff, *Institutions and Technological Innovation During Early Economic Growth: Evidence form the Great Inventors of the United States, 1790–1930*, at 21–22 (CESifo, Working Paper No. 1299, 2004).

[278] Nicholas Bloom, Mark Schankerman & John Van Reenen, *Identifying Technology Spillovers and Product Market Rivalry* (Nat'l Bureau of Econ. Research, Working Paper No. 13060, 2007), http://eprints.lse.ac.uk/780/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Centre_for_Economic_Performance_Discussion_papers_dp0675%20(2).pdf.

[279] Charles Tait Graves & James A. DiBoise, *Do Strict Trade Secret and Non-Competition Laws Obstruct Innovation?*, 1 ENTREPRENEURIAL BUS. L.J. 323, 339 (2006).

in their field of expertise than risk civil liability. When the stakes involve the possibility of criminal liability, such avoidance is all the more likely. And it is not only the defendants who are affected. Increased trade secret litigation against former employees also means that other employees and co-workers who have witnessed such disputes, are discouraged from pursuing professional opportunities.[280] Indeed in some cases, litigation against a former employee-turned-competitor is primarily meant to send a warning signal to all employees in the firm. As Rosemary Ziedonis and her co-authors put it, "[e]ven if the costs of being litigious in a particular dispute outweigh the benefits, the deterrence of future knowledge spillovers can justify the investment."[281]

Entrepreneurship is at particular risk. Employees are far more likely to pursue entrepreneurial activities the greater their professional ties, yet as we saw, trade secret litigation can reduce the density of relationships.[282] Moreover, while large incumbent firms can sometimes mitigate the risk of prosecution by erecting walls,[283] so that a new employee is segregated from those working on projects that compete with a former employer, that strategy is not practical—or is absolutely impossible—for start-ups, which may have few workers and only one major project. In addition, incumbents with large resources are better situated to offer their employees indemnification to protect them from legal liability and to defend against trade secret litigation. As we saw, they can also use their superior resources to drive out competition.[284] Start-ups have none of these advantages. Finally, the threat of litigation can dry up the venture capital investment start-ups need to develop their products, launch them, and become successful.[285]

Exacerbating the problem is the expansion of the EEA to cover "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, elec-

---

[280] Martin Ganco, Rosemarie H. Ziedonis & Rajshree Agarwal, *More Stars Stay, but the Brightest Ones Still Leave: Job Hopping in the Shadow of Patent Enforcement*, 36 STRATEGIC MGMT. J. 659 (2015).

[281] Rajshree Agarwal, Martin Ganco & Rosemarie H. Ziedonis, *Reputations for Toughness in Patent Enforcement: Implications for Knowledge Spillovers via Inventor Mobility*, 30 STRATEGIC MGMT. J. 1349, 1354 (2009).

[282] Ramana Nanda & Jesper B. Sørensen, *Workplace Peers and Entrepreneurship*, 56 MGMT. SCI. 1116 (2010).

[283] The EEA gives the term "Chinese wall" new meaning.

[284] Patrick Bolton & David S. Scharfstein, *A Theory of Predation Based on Agency Problems in Financial Contracting*, 80 AM. ECON. REV. 93 (1990).

[285] Alexander E. Silverman, Symposium Report, *Intellectual Property Law and the Venture Capital Process*, 5 HIGH TECH. L.J. 157 (1989).

tronically, graphically, photographically, or in writing."[286] Particularly when the subject matter involves complex technical information, prosecutors and courts likely defer to companies' self-definition of proprietary information, and companies have expanded the subject matter of proprietary information to include virtually everything.[287] Evidently, then, any type of information can now qualify as confidential. As a result, former employees may face charges at almost any turn if they choose to continue in their field of their expertise and compete with their former employer.

Employers recruiting new talent are also at risk. The EEA defines as a criminal not only the individual who takes the trade secrets but also third parties, namely competitors or anyone who "receives, buys, or possesses a 'trade secret,' knowing the same to have been stolen or appropriated, obtained, or converted."[288] The perverse result is that employers are most at risk to be in violation of the EEA when they logically choose to hire the most experienced employees—people who have already worked in the industry and gained invaluable training.[289] The bottom line is that, today, hiring employees away from competitors inevitably entails a threat of criminal sanctions. With reduced willingness to hire experienced knowledge workers comes a significant decrease in knowledge flows across firms, reduced employment opportunities, and a dampened desire to enter the technology sector.

---

[286] 18 U.S.C. § 1839(3)(2012).

[287] For example, Google's standard contract for new employees includes the following definition: "*Confidential Information* means, without limitation, any information in any form that relates to Google or Google's business and that is not generally known. Examples include Google's non-public information that relates to its actual or anticipated business, products or services, research, development, technical data, customers, customer lists, markets, software, hardware, finances, employee data and evaluation, trade secrets or know-how, intellectual property rights, including but not limited to, Assigned Inventions (as defined below), unpublished or pending patent applications and all related patent rights, and user data (i.e., any information directly or indirectly collected by Google from users of its services). Google Confidential Information also includes any information of third parties (e.g., Google's advertisers, collaborators, subscribers, customers, suppliers, partners, vendors, partners, licensees or licensors) that was provided to Google on a confidential basis." Google Employment Contract (on file with authors).

[288] 18 U.S.C. §§ 1831(a)(3), 1832(a)(3).

[289] There may well be systemic gender and age impact. Women are still more likely than men to be geographically constrained because of dual careers and when facing the risks of trade secret claims, may choose more frequently to either not leave their employer in search of a better position or to drop out of the job market for some time and devote themselves to care work at home. Similarly, older employees are likely to have more job experience, which perversely, under the new cognitive property, creates a further penalty on their employment, in a labor market that is already prone to age discrimination. *See* Noam Scheiber, *The Brutal Ageism of Tech*, NEW REPUBLIC (Mar. 23, 2014), http://www.newrepublic.com/article/117088/siliconsvalleys-brutal-ageism.

IV. RECONCILING LEGITIMATE INTERESTS

None of this is to say that the FBI—or the government more generally—should not be concerned about cyber terrorism or even about international trade secret violations. We do not advocate abolishing the EEA. We do, however, recommend several changes in the trade secret regime.

Clearly, it would be helpful to amend the EEA to expressly incorporate many of the limits that cabin tort actions and ensure that knowledge workers can enter into fruitful exchanges and employees can retain the ability to move between jobs. The statute should make clear that subjective intent is not enough and that the victim's characterization of information as proprietary is not controlling. The information taken must, from a rational perspective, be a trade secret whose unauthorized taking could harm its owner.[290] The other elements—what counts as an unauthorized taking, the degree to which information can retain its status as a secret despite the industry's knowledge of it, the kinds of harm that are actionable—should also be defined more precisely. In addition, thought might be given to delineating the kinds of information that are protectable through criminal law. Trade secret theft should be carefully distinguished from cyber-hacking. Both can be accomplished electronically, but hacking is designed to destroy infrastructure important to all aspects of public life; it has a very different social impact from theft in the private realm. Similarly, the law would benefit from the classification system used in the NSD-189 context: the taking of military or dual-use information is categorically different from the code Goldman Sachs uses when it gains an edge in the stock market through high-frequency trading; arguably, criminal prosecution should be limited to the cases involving the strongest national interests.

It is particularly important to clarify the acts that are sufficient to give rise to charges of attempt or conspiracy. Within the creative industries, there are many acts that are common yet, in retrospect, can be made to look suspicious. After all, programmers routinely keep copies of files they worked on, store information on servers in unknown locations,[291] or use one another's passwords;[292] similar activities go on in other professional settings (including law firms). And as we saw, the government even regards some very conventional academic events (conferences, meetings

---

[290] At the very least, it behooves prosecutors to understand that everything that looks technologically complex is not a trade secret. *See, e.g.*, Apuzzo, *supra* note 247 (noting that a case against Xi Xiaoing, chair of the physics department at Temple University, was dropped after world-renowned physicists submitted affidavits stating that the technology he discussed in emails was not restricted).

[291] *See* Lewis, *supra* note 145 (noting the activities regarded as suspicious in the Aleynikov case).

[292] *See* Perlroth, *supra* note 179 (describing the actions for which Chen is now being fired).

with foreigners, travelling back and forth between your home country and country of residence) as suspicious.[293] It is certainly easy to understand the need to preserve the government's ability to mount sting operations that involve the passage of fake secrets (as occurred in *The Company Man*). But because attempt and conspiracy charges have no analogue in civil trade secret law, there is a special need to be clear that not every suspicious act can constitute the basis for these offenses. To date, the EEA has not been successfully challenged as void for vagueness.[294] However, judging from the aggressive positions taken in the IP Crimes Manual, the statute fails to provide adequate notice of what the government considers a crime.

Much the same can be said of the provision extending the EEA extraterritorially whenever "an act in furtherance of the offense was committed in the United States."[295] In recent years, the Supreme Court has been skittish about extending U.S. law too broadly as the imposition of American law can interfere with the sovereign authority of other countries and disrupt international relations.[296] Superficially, the EEA fulfills the Court's requirement that Congress express the view that the law apply to foreign activity. Congress may not, however, realize the sorts of activities the government regards as suspicious. Clarification would therefore be useful from both a local and international perspective.

In addition to focusing on the EEA itself, there is a need to consider the cumulative effect of government responses to the threat of trade secret misappropriation. The double prosecution of Aleynikov, including the New York prosecutor's use of concepts developed in the federal case,[297] raises questions about the relationship between the federal and state attorneys. Given that the Second Circuit took the unusual step of reversing Aleynikov's conviction and ordering him acquitted and released immediately,[298] the rapidity of the second indictment less than six months later had vindictive overtones that alone raise conspiracy theories. The impending federal civil law is also problematic. Because it is not meant to preempt state law, a federal right of action would introduce yet another layer of protection and expose the technological community to the possibility of four separate lawsuits over the same activity. As others

---

[293] *See supra* notes 109–116 and accompanying text.

[294] *Cf.* Johnson v. United States, 135 S. Ct. 2551 (2015) (requiring criminal statutes to give adequate notice of the conduct to be punished).

[295] 18 U.S.C. § 1837(2) (2012).

[296] *See, e.g.*, Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659 (2013).

[297] *See* Lewis, *supra* note 145, at 23 (describing the New York prosecutor's use of a phrase originally from the opening statement of Aleynikov's lawyer in the federal case).

[298] *See* Aleynikov v. Goldman Sachs Grp., Inc., 765 F.3d 350 (3d Cir. 2014).

have noted, the result will be greater uncertainty, less mobility, and an even greater chill on creative production.[299]

But rethinking enforcement is not enough. It is equally crucial to reconsider the rhetoric equating trade secrecy with national security. The climate generated by an approach that seeks to stanch the flow of information is not in the long term national security interest of the United States. Vigorous enforcement of the EEA may protect the current technological position of the United States (in that indirect sense, it is perhaps a national security issue, just as is any national economic policy). However, it also handicaps the nation's ability to foster creative communities that can continue to engage in sophisticated, imaginative research at the highest technological levels. Local incumbents may thus retain their positions for longer, but a system that discourages academic research, startups, global talent recruitment, and job mobility is not one that will perpetuate the dominance of U.S. innovation in the global economy.

The national security trope also undermines intellectual property values. In particular, it ignores a core principal of all intellectual property regimes: that protection is intended only to allow innovators to recoup their investment and earn enough profit to encourage more innovation.[300] Exclusivity is not meant to be permanent; it is not a goal in itself but rather a means for producing dynamic efficiency. Copyright and patent laws protect innovators from free riders only for specified periods of time, after which the protected advances fall into the public domain, where they can be freely used and improved upon.[301] The trade secret regime has no counterpart to a specific term of years. Instead, it relies on leakage—reverse engineering and independent invention to be sure, but also leakage through interactions within the creative sector.[302] Unless those enforcing the EEA understand the potential impact of reducing this leakage, enforcement will destroy an important accommodation between proprietary and access interests. Knowing their trade secrets will be vigorously enforced courtesy of the government could also alter the choice innovators make between trade secrecy and patent protection. In a worst case scenario, it may lead inventors to alter their research agendas

[299] *See* Argento, *supra* note 183, at 172; Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015); *see also* David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015).

[300] Hugo A. Hopenhayn & Matthew F. Mitchell, *Innovation Variety and Patent Breadth*, 32 RAND J. ECON. 152 (2001).

[301] *Id.* at 153.

[302] Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L REV. 1803, 1805–06 (2014).

so that the advances they discover can be kept in a domain where others can never benefit from them.[303]

It is also worth considering the effect of specific claims that support the new rhetoric. As the Chen case suggests, not all foreigners, or even all foreigners who return to their birthplace for visits, are intent on stealing the fruits of American ingenuity. That mindset represents racial profiling at its most pernicious.[304] It also produces spectacular prosecutorial errors, including investigations and indictments that fall apart, but nonetheless do significant damage to the people involved.[305] Furthermore, the rhetoric injures the innovation environment. There is a deep literature on the Not-Invented-Here syndrome, which shows that firms willing to collaborate and transact with others are more successful and produce more impactful inventions than firms that reject advances that are not invented internally.[306] It is ironic (if not tragic) that just as U.S. industry has largely shaken off this syndrome, the EEA not only invigorates it, but also transposes it into a geographical realm, so that it is no longer possible to accept inputs from scientists who were not born in the United States.

Similarly, there are significant questions about the extent of that $400 billion—the figure *The Company Man* mentions as the loss U.S. industry is experiencing each year. It is clearly wrong to measure it by looking at the cost to development. As we argued above, a significant part of public funding is intended to produce public knowledge. Utilizing the advances made possible with NSF funding is not theft if the NSF intended the recipient researchers to publish what they learned. Furthermore, not all investment in development results in inventions or in commercializable products. Nor should loss be evaluated according to the price the inventor wishes to charge customers. The use the United States makes of that measure has been rejected in international disputes for the very good reason that it ignores the demand function—that is, whether those who could use the product productively will actually buy it at the manu-

---

[303] Nor can the government regulate them for safety, environmental, or health concerns. *See, e.g.*, Mary L. Lyndon, *Secrecy and Access in an Innovation Intensive Economy: Reordering Information Privileges in Environmental, Health, and Safety Law*, 78 U. COLO. L. REV. 465 (2007).

[304] To some extent, rethinking has begun. *See* Perlroth, *supra* note 199 (describing a congressional request that the Department of Justice review whether race played a role in espionage investigations).

[305] *See, e.g.*, Joyce Xi, *To Get My Father, Xiaoxing Xi, FBI Twisted America's Ideals*, USA TODAY (Sept. 20, 2015), http://www.usatoday.com/story/opinion/2015/09/18/xiaoxing-xi-china-spy-fbi-state-visit-column/32560009/ (describing the problems that the failed prosecution of Xiaoxing Xi inflicted on the author's family).

[306] *See, e.g.*, Ajay Agrawal, Iain Cockburn & Carlos Rosell, *Not Invented Here? Innovation in Company Towns*, 67 J. URB. ECON. 78 (2010); Ralph Katz & Thomas J. Allen, *Investigating the Not Invented Here (NIH) Syndrome: A Look at the Performance, Tenure, and Communication Patterns of 50 R & D Project Groups*, 12 R&D MGMT. 7 (1982).

facturer's suggested retail price.[307] Apart from international concerns with this calculation, there are several domestic contexts in which a more realistic approach to damages is being taken, including awarding damages in a patent case,[308] sentencing white-collar criminals,[309] and imposing punitive damages.[310] The current rhetoric of trade secrecy flies in the face of these trends. Besides, even if there are significant costs associated with theft, the ambiguous effect of the law suggests that the costs of enforcement and the social benefit of spillovers should also be considered in determining the net effect of theft of economic welfare.

Equating trade secret protection with national security also works at cross-purposes with other government initiatives. As Burstein showed, enhancing industry's ability to enforce trade secrets that are lost undermines private firms' incentives to protect their technologies themselves.[311] The prosecution of employees who wish to found their own firms[312] runs counter to the attention the U.S. Small Business Administration lavishes on encouraging start-ups,[313] which it views as a core component of na-

---

[307] *See* Panel Report, *China—Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, ¶ 7.465–468, WTO Doc. WT/DS362/R (adopted Jan. 26, 2009) (adopting a measure based on the prices at which customers bought unauthorized copies). In agreements subsequent to TRIPS, however, the United States has managed to insert its view. *See, e.g*, Anti-Counterfeiting Trade Agreement arts. 9(1), 23(1), Dec. 3, 2010, *opened for signature* Mar. 31, 2011, 50 I.L.M. 243 (noting that "commercial activities for direct or indirect economic or commercial advantage" are included and that and the calculation of loss is to be based on "any legitimate measure of value the right holder submits, which may include lost profits, the value of the infringed goods or services measured by the market price, or the suggested retail price").

[308] *See* Lucent Techs., Inc., v. Gateway, Inc., 580 F.3d 1301 (Fed. Cir. 2009).

[309] *See* Derick R. Vollrath, Note, *Losing the Loss Calculation: Toward a More Just Sentencing Regime in White-Collar Criminal Cases*, 59 DUKE L.J. 1001, 1018–20 (2010).

[310] *See* Laura J. Hines & N. William Hines, *Constitutional Constraints on Punitive Damages: Clarity, Consistency, and the Outlier Dilemma*, 66 HASTINGS L.J. 1257 (2015).

[311] *See supra* text accompanying notes 157–161.

[312] An example of the first situation, using proprietary information to start a solo venture, is in Indictment, United States v. Newman, No. 1:14-cr-00704 (N.D. Ill. Dec. 4, 2014). The indictment alleges that a stock trader for "Trader Firm" accessed and copied more than 400,000 computer files onto a thumb drive (information including algorithms, source code, and executable files). *Id.* at 3–4. The same month, February 2014, Newman created his own company, "NTF LLC" which signed an agreement with CME online trading platforms. *Id.* at 4. In March 2014, Newman resigned from Trading Firm and established a trading account for NTF LLC. *Id.* at 5. The indictment alleges that Newman stole various trade secrets from Trading Firm, which he then used to support his solo venture. Specifically the indictment notes a "proprietary computer file used for pricing commodity futures contracts." *Id.* As of February 21, 2015, this action is pending in the Northern District of Illinois.

[313] *See, e.g., Startup in a Day*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/about-sba/sba-initiatives/startup-day (noting actions to reduce the effort required to start a firm).

tional innovation strategy.[314] The chill imposed on leaving a firm to start a new one also interferes with the goals of the 2012 JOBS Act,[315] which sees start-ups as an important part of a strategy to increase employment. Recent changes in patent law have analogously reflected the importance of encouraging small businesses to become entrepreneurial.[316]

Paradoxically, the same industries that decry the loss of secrets to foreign countries are simultaneously concerned about a talent drought—a shortage that the technology industry claims "could endanger U.S. competiveness as Canada, Germany, South Africa and China attempt to woo engineers from abroad too."[317] Worried about the venture investments that Chinese companies have made in entrepreneurs around the world, and that the Silicon Dragon will pose a serious threat to Silicon Valley, these industries have lobbied for the 2015 Immigration Innovation Act, a bill which increases the cap on H-1Bs and is designed to help the tech industry address this talent shortage.[318] But aggressive prosecution of foreign nationals cuts directly against such attempts to win the global brain-drain battles.

Consider also the Fulbright Program. It was initiated in 1946 by Senator J. William Fulbright to strengthen the basis for peace by promoting mutual understanding between the people of the United States and the peoples of partner countries around the world. The Fulbright fellowship is the U.S. government's flagship academic exchange program. It operates in more than 155 countries. Each year, it grants approximately 4,000 foreign students scholarships and awards travel funds to almost 2,000 American academics.[319] A central requirement attached to a foreign receipt of a Fulbright fellowship is to return to one's home country for at least two years after studying in the United States in order to impart the wisdom learned here abroad.[320] At the same time, however, the extensive publicity given to EEA cases involving academics, such as the charges against Beijing academics at Tianjin University, conveys the opposite message: Do not expect to return to your country with knowledge you

---

[314] *See id.*

[315] Jumpstart Our Business Startups Act, Pub. L. No. 112-106, 126 Stat. 306 (2012).

[316] *See, e.g.*, 35 U.S.C. § 41(h) (2012); 37 C.F.R §§ 1.27–1.29 (2014) (fee reductions for micro-entities and other small entities); 35 U.S.C. § 273 (2012) (recognizing prior user rights to protect non-patentees who are first users).

[317] Katie Benner, *Obama, Immigration and Silicon Valley*, BLOOMBERG VIEW (Jan 22, 2015), http://www.bloombergview.com/articles/2015-01-22/obama-immigration-reform-h-b1-visas-and-silicon-valley.

[318] Press Release, Mark R. Warner, Sens. Warner & Kaine Introduce Bipartisan Startup Act (Jan. 16, 2015), http://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=75c06654-ae4c-4d39-b9bd-b8bf3bbc399e.

[319] *See The Fulbright Program: Facts and Common Questions*, BUREAU EDUC. & CULTURAL AFF., http://eca.state.gov/fulbright/facts-and-common-questions.

[320] *See id.*

gathered. It is sure to discourage foreigners from visiting, studying—or, eventually, working in the United States and contributing their talents to the American economy.[321]

CONCLUSION

In many ways, reframing trade secret theft as a national security issue is understandable. Cyber warfare is clearly increasing and the FBI needs all the help it can get in identifying hackers and other high tech terrorists. Furthermore, there is plenty of secret information with critical military uses; protecting that material is certainly in the nation's best interest. However, the rhetoric surrounding economic espionage goes well beyond these well-recognized arenas. It would extend protection to technology that is not clearly secret (as in the Liu and Jin cases) or valuable (as with Aleynikov), and that is only of private concern (as with many of the technologies mentioned in the government reports). It throws suspicion on collaboration, joint ventures, academic exchanges, establishing new companies, and switching jobs.

Without prosecutorial sensitivity to intellectual property values, along with a more nuanced view of the contributions foreign innovators make to domestic inventiveness, creative development will suffer. Not only will the country fall behind globally, it will be harder to produce the advances necessary to address new threats, many of them inherently global—climate change and pollution, Ebola and other new diseases, and resistance to antibiotics, to name a few. In the name of preserving U.S. technological dominance, overblown trade secret law can deter the very conduct that would, in fact, maintain the United States' leadership in the innovation sector.

To be sure, there is a trade-off here. While greater openness and more vigorous opportunities to share information and learn from others would lead to more technological progress, they could also expose valuable information. But even from a pure security angle, the zealous approach to trade secrecy is problematic. This approach undermines the dynamic goals of intellectual property law to promote future innovation. It contradicts the view of the United States as a benign world leader, helping countries reach development and democratization, through education and progress, trade, investment, and aid. It ignores the United States' own history of progress and prosperity, which, as historian Doron Ben-Atar has, shown, was heavily dependent on the misappropriation of trade secrets from the Old World. It is, as Ben-Atar concluded, "impossible to contain the abuse of technology without undermining the free

[321] Chun Han Wong, *Economic Espionage Charges Could Further Dent China–U.S. Ties*, WALL ST. J. (May 22, 2015), http://www.wsj.com/articles/economic-espionage-charges-could-further-dent-china-u-s-ties-1432135288.

flow of knowledge that is the prerequisite for innovation."[322] It has always been the case that we understood innovation and global economic development as the key to security and world peace. Terrorism and extremism are, after all, fed by poverty and ignorance.

[322] Doron Ben-Atar, *Hollywood Profits v. Technological Progress*, CHRON. HIGHER EDUC. (Apr. 1, 2005).