Northwestern Journal of Technology and Intellectual Property

Volume 12 | Issue 4 Article 1

2014

More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership

Andrew F. Popper
American University, Washington College of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership

Andrew F. Popper

November 2014 VOL. 12, NO. 4

Northwestern Journal of Technology and Intellectual Property
Volume 12, Number 4 (November 2014)

More than the Sum of All Parts: Taking on IP and IT Theft Through a Global Partnership

By Andrew F. Popper*

The core of this Article describes some of the efforts, both within and outside the United States, to control the epidemic of intellectual property and information technology (IP and IT) theft. Those engaged in the battle include prosecutors and judges, individuals and trade associations, and politicians and policymakers from all points on the political spectrum. And yet, even with so many forces working to stem the tide, the losses are staggering.

An innovator with the potential to change his or her future as well as the prosperity of the surrounding economy, whether in Kentucky or Kinshasa, will be dissuaded from innovating if that which they invent or produce is readily stolen. Individual and governmental enforcement efforts are making a difference, but success in dealing with this problem does not lie in any one or even several approaches. Instead, there is a need for coordinated and collective efforts, harnessing domestic and international resources. The enforcement and control mechanisms discussed in this Article show the power and limits of each approach. Taken in the aggregate, however, there is reason to think a global change is possible. In a word, the solution lies in partnership.

Through constant and transparent dialogue and the sharing of ideas and resources, a partnership has the potential to reverse the rate and impact of IP and IT theft. It may be the only way to begin the process of achieving the most important goal: a cultural shift resulting in universal condemnation of entities and individuals engaged in piracy, counterfeiting, and other forms of IP and IT theft.

TABLE OF CONTENTS

* Professor of Law, American University, Washington College of Law. Great thanks are due to talented American University Washington College of Law research assistants: Chelsea Zimmerman, Christin Mitchell, Kelly Brouse, Tracy Beinenfeld, and Catherine Riedo. Many thanks also to Dean Claudio Grossman for his encouragement and support, and to Microsoft Corp. for assistance funding research assistants.

I. INTRODUCTION

¶1 This Article describes some of the efforts, both within and outside the United States, to control the epidemic of intellectual property and information technology (IP and IT) theft. Those engaged in the battle include prosecutors and judges, politicians and policymakers from all points on the political spectrum, domestic and multinational organizations, state and federal officials, representatives of the executive branch and independent agencies, individual litigants, and more. And yet, even with so many forces working to stem the tide, the losses are staggering.

¶2 An innovator with the potential to change his or her future as well as the prosperity and success of the surrounding economy, whether in Kentucky, Kinshasa, Kazakhstan, or Kansas, will be dissuaded from innovating if that which they invent or produce is readily stolen. It is thus worth considering how the wrongfulness of outright IP and IT theft can be isolated and condemned, and then, how that condemnation can be communicated. Complex single-case enforcement actions in the United States or elsewhere, while absolutely essential, are not likely to be table-talk at the evening meal in most quarters. Public communication of an obvious but somehow ignored or flouted truth—that stealing valuable property is simply wrong, even though such theft has been made easier and more anonymous by modern technology—must be part of the solution to IP and IT theft.

¶3 Individual and state-level efforts are making a difference, but success in dealing with this problem does not lie in any one or even several approaches. Instead, there is a need for coordinated and collective efforts, harnessing domestic and international resources. The enforcement and control mechanisms discussed in this Article show the power and limits of each approach. Taken in the aggregate, however, there is reason to think a real and global change is possible. In a word, the solution lies in partnership. In every sense of the term, partnership holds the potential for a meaningful diminution of IP and IT theft.

¶4 For state enforcement, one of the recent shining lights in this field, jurisdictional issues will not be easily resolved. Enforcement outside of local court orders and the limited scope of remedies will remain a problem. Enforcement of federal statutory and regulatory claims also presents an opportunity to lessen IT and IP piracy and cybercrimes, but there are still inherent limits in statutes, uneven enforcement, unresolved matters relating to extraterritoriality, and of course problems marshaling sufficient political will and resources.

¶5 International and multinational organizations also hold promise but are plagued with many of the same problems faced by state and federal entities.[1] The World Trade Organization[2] and similar institutions committed to articulating and enforcing standards lack reliable and consistent juridical force. Moreover, efforts by international groups are hampered by the variation in enforcement will and resources between developing and emerging countries and the differences from country to country in (or nonexistence of) legal regimes for protecting IP and IT.

¶6 Finally, there are private organizations, including individual companies, trade and other professional organizations, and domestic and multinational alliances, all dedicated to stemming the tide of intellectual property theft. Like the governmental entities described above, the will and motives are strong but the enforcement mechanisms and resources needed to make meaningful change are limited.[3] Throughout this Article, I reference select efforts of organizations and entities to orchestrate a campaign to stop IP theft. All are laudable and have good intentions. Yet none has succeeded; none is truly global; and none effectively merges public and private resources.[4]

¶7 In this environment, the most logical way to think about the problem of IP and IT theft boils down to partnership. One commentator noted that meaningful protection of IP and IT is a legal and cultural undertaking that will involve "thousands of detailed actions—data gathering and research, interagency coordination, work with the private sector, coordination with Congress, and interactions with foreign government agencies. This work must be done by expert officials across many departments and agencies working together in interagency teams with a great deal of private-sector outreach."[5]

---

[1] There are a number of international organizations dedicated to protecting the rights of those who produce IP and IT. None have the reach, juridical force, resources, membership, reliable enforcement mechanisms, and other features of a true multidimensional transnational partnership. *See*, *e.g.*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/portal/index.html.en (last visited Sept. 6, 2014); GLOBAL INTELLECTUAL PROP. CTR., U.S. CHAMBER OF COMMERCE, http://www.theglobalipcenter.com/about/mission-and-goals/ (last visited Sept. 6, 2014) (focusing on raising awareness and "increasing support among key audiences"); INT'L ASS'N FOR THE PROTECTION OF INTELLECTUAL PROP., https://www.aippi.org/?sel=aims (last visited Sept. 6, 2014) (discussing goals dedicated to development and improvement of regimes to protect IP); INT'L INTELLECTUAL PROP. INST., http://iipi.org/2010/07/background/ (last visited Sept. 6, 2014) (providing education and guidance for national leaders, particularly in developing countries).

[2] WORLD TRADE ORG., http://www.wto.org/ (last visited Jan. 29, 2014).

[3] The closest to the model proposed in this Article is the International Intellectual Property Alliance (IIPA). *See About IIPA*, http://www.iipa.com/ (last visited Sept. 6, 2014). Founded in 1984, the IIPA has tried for three decades, with only limited success, to develop rules and policies to protect IT and IP. It is a "private sector coalition . . . [with] over 3,200 U.S. companies . . . Members [include the] Association of American Publishers, Entertainment Software Association, Independent Film & Television Alliance, Motion Picture Association of America, National Music Publishers' Association, and Recording Industry Association of America." *About IIPA*, http://www.iipa.com/aboutiipa.html (last visited Sept. 6, 2014). It does not include the entire array of public-sector members needed to achieve the goals set out in this Article.

[4] The partnership between the National Crime Prevention Council and the Justice Department's Bureau of Justice Assistance is an example of a public/private partnership that offers potential remedies, but thus far has had few identifiable results. *Intellectual Property Theft: Get Real*, NAT'L CRIME PREVENTION COUNCIL, http://www.ncpc.org/topics/intellectual-property-theft/ncpcs-intellectual-property-theft-campaign (last visited Sept. 5, 2014) ("Because intellectual property theft is so harmful, the National Crime Prevention Council, in partnership with the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, has launched a campaign to show how harmful it is—to all of us—and to help prevent it. Research shows that when people know the costs—and the dangers—of intellectual property theft, they take it much more seriously.").

[5] DENNIS C. BLAIR ET AL., NAT'L BUREAU OF ASIAN RESEARCH, THE IP COMMISSION REPORT: THE

¶8 Through constant and transparent dialogue and the sharing of ideas and resources, a partnership has the potential to reverse the rate and impact of IP and IT theft.[6] It may be the only way to begin the process of achieving the most important goal: a global change in fundamental beliefs resulting in a universal condemnation of IP and IT theft.

II. THE IMPACT AND NATURE OF IP AND IT THEFT

A. Supply-Chain Basics and Nondisclosure Agreements

¶9 Research for this Article began with a study of supply chains and the hope of discerning the means, within a supply chain, to curtail IP and IT theft. Most products require and benefit from identifiable supply chains, and very few are exclusively local. Typically, an end-product comes to market as the result of varying forms of collaboration between multiple domestic and foreign actors functioning within a supply chain.[7]

¶10 Most items in commerce begin with conceptualization, or IP of one type or another, followed by raw-product selection and initial fabrication, processing and assembly of component parts, unit assembly, packaging, and sale. It is highly likely that one or more of these activities occurs abroad.[8] Effective product development and assembly along this chain often requires creation, transmission, and in effect, entrustment of valuable IP and IT to both domestic and foreign entities. In that process, control over IT and IP within the supply chain is essential, efficient, and bears inherent risk.

¶11 In one sense, supply chains provide a vehicle to protect IP and IT, and in another, pose a vulnerability because of multiple actors with varying allegiances and motives. "The globalization of the supply chain for new—and increasingly interconnected—IT products will offer more opportunities for malicious actors to compromise [product] integrity and security."[9]

¶12 At first blush, the supply chain seems a safe haven where, for generations, basic nondisclosure agreements (NDAs) were used to protect IP and IT. However, NDAs can be ineffective, difficult and expensive to enforce, and cannot resolve the disclosure paradox that potentially exists between innovators, producers, and purchasers of the product.[10] The haunting notion of an intellectual-property paradox cannot easily be

---

REPORT OF THE COMMISSION ON THEFT OF AMERICAN INTELLECTUAL PROPERTY 63 (2013) [hereinafter IP COMMISSION REPORT], *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

[6] One example of an attempt to coordinate multiple public and private actors is the Extractive Industries Transparency Initiative, "a global coalition of governments, companies and civil society working together to improve openness and accountable management of revenues from natural resources." *What Is the EITI?*, http://eiti.org/eiti (last visited Sept. 6, 2014).

[7] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-361, IT SUPPLY CHAIN: NATIONAL SECURITY RELATED AGENCIES NEED TO BETTER ADDRESS RISKS 4 (2012), *available at* http://www.gao.gov/assets/590/589568.pdf.

[8] *See* CTR. FOR RESPONSIBLE ENTER. & TRADE, IP THEFT: REPORT HIGHLIGHTS SUPPLY CHAIN VULNERABILITIES (2013) [hereinafter CTR. FOR RESPONSIBLE ENTER. & TRADE, IP THEFT].

[9] EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 7 (2013) [hereinafter ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS], *available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[10] Jonathan M. Barnett, *Intellectual Property as a Law of Organization*, 84 S. CAL. L. REV. 785, 798 (2011).

dismissed and is not limited to the critique of NDAs. At its most basic level, the paradox is predicated on the necessary disclosure of information (necessary to protect IP and IT), and the presence of those within and with access to some aspect of a supply chain anxious to use but unwilling to pay for IP and IT.[11] "NDAs typically protect against subsequent disclosure by the idea buyer to third parties, but not use by the idea buyer."[12] While normally this paradox focuses on the innovator and the purchaser of the idea, this also has implications for IP and IT theft throughout any supply chain.

¶13 If one assumes a societal willingness to steal and an historic unwillingness of some governmental entities, within and outside the United States, to expend resources to prosecute such theft, deterrence is stymied, and simple NDAs—or even complex judicial and administrative remedies for IP and IT theft—will not reliably protect the rights of owners. Similarly, while coding requirements and comparable protection measures (from passwords to complex, access-limitation algorithms) have historically provided some protection for software IP owners, such safeguards have not thwarted technology-savvy IP thieves.[13] More is required. How much more ought to be driven by the sheer economic impact of IP and IT theft.

B. Impact of IP and IT Theft

¶14 Descriptions of the consequences of IP and IT theft vary only in amount. "Pirated software and other stolen intellectual property . . . affects every corner of an American economy . . . ."[14] IP and IT "are two major drivers of U.S. economic growth and prosperity [and] cyber attacks threaten both."[15] The Organization for Economic Co-operation and Development (OECD) estimated that cross-border trade in physical counterfeits and pirated products alone reached a value of $250 billion in 2007, representing a fraction of the scope and impact of IP violations worldwide.[16]

¶15 It stands to reason that if those who invest money, time, and energy to create or invent different, better, and more efficient products cannot rely on IP and IT protection of their rights, their willingness to engage in this vital economic activity will decline. "Yet as bad as the economic and employment losses are, the OECD Commission notes that IP theft's most insidious impact lies in undermining both the incentives and means to invest in innovative activity."[17]

---

[11] For example, a patent discloses to the public the secrets of the invention. Those inclined to steal that information have their tasks as thieves made easier by the public filings patent protection requires.

[12] Barnett, *supra* note 10, at 798.

[13] *See* Yogesh Malhotra, *Controlling Copyright Infringements of Intellectual Property: The Case of Computer Software—Part One,* 45 J. OF SYS. MGMT. 32 (1994) ("Most technological solutions devised to prevent unauthorized copying of computer software have provided only temporary protection against software theft.").

[14] Rob McKenna, *Defending U.S. Intellectual Property*, WASH. TIMES (Apr. 26, 2013), http://www.washingtontimes.com/news/2013/apr/26/defending-us-intellectual-property/?page=all.

[15] John Dowdy, *The Cybersecurity Threat to U.S. Growth and Prosperity*, *in* SECURING CYBERSPACE: A NEW DOMAIN FOR NATIONAL SECURITY 129, 134 (Nicholas Burns & Jonathon Price eds., 2012).

[16] DANIEL SANDY BAYER, RONALD E. BERENBEIM, & REBECCA WALKER, SAFEGUARDING INTELLECTUAL PROPERTY AND ADDRESSING CORRUPTION IN THE GLOBAL SUPPLY CHAIN 11, 13, 19, 30, 36, 47 (2012).

[17] Stephen Ezell, *Stop Thief! Time to Limit US IP Theft*, THE HILL'S CONG. BLOG (June 10, 2013, 2:00 PM), http://thehill.com/blogs/congress-blog/technology/304231-stop-thief-time-to-limit-us-ip-theft-.

¶16 A well-funded global partnership of prosecutors, politicians, policymakers, domestic and multinational organizations, state and federal officials, and representatives of the executive branch and independent agencies—the enforcement cohort mentioned at the outset of this Article—could formulate a strategy to begin to undo the belief that it is acceptable to steal, whether by downloading, file-sharing, or other forms of piracy.

¶17 Various organizations[18] and academicians alike argue that the losses sustained are either exaggerated or inconsequential.[19] I disagree. By any measure, piracy accounts for billions of dollars in lost value,[20] which leads to three conclusions. First, IP and IT theft exact an enormous cost on the U.S. and global economy. Second, the means to prevent such theft are limited and ineffective given the magnitude of the problem.[21] Third, there is little agreement between commentators on the best way to calculate or describe the magnitude of the loss.

¶18 The International Trade Commission (ITC)[22] estimated that in 2009, the American IP-intensive economy lost "$48.2 billion in sales, royalties, or license fees due to IPR infringement in China" alone.[23] A study focused solely on software estimates that "the global piracy rate for PC software hovers at 42 percent," and the "commercial value of this shadow market of pirated software climbed from $58.8 billion in 2010 to $63.4 billion in 2011, a new record, propelled by PC shipments to emerging economies where piracy rates are the highest."[24]

¶19 In the U.S. economy, IP and IT accounts for "40 percent of the U.S. GDP, 74 percent of U.S. exports, and supports over 40 million U.S. jobs."[25] The Director of the National Security Agency reported that IT and IP theft exacts an annual cost of $320 billion and is responsible for the loss of millions of jobs, declaring this ongoing theft the "greatest transfer of wealth in history."[26] Given the enormity of these losses, a reduction of piracy by merely ten percent over four years in California alone would "generate over

[18] This Article is premised on the belief that protection of IP and IT is fundamental to healthy economies and essential for sustained invention, creativity, and innovation. There are those who take the position that IP and IT are overprotected and that the real challenge in this field is to ensure information transparency to free up IP and IT to the public. Organizations like the Global Network Initiative pursue this goal, taking the position that "domestic laws and policies [protecting IP and IT] may conflict with the internationally recognized human rights of freedom of expression and privacy." GLOBAL NETWORK INITIATIVE, http://www.globalnetworkinitiative.org/ (last visited Jan. 26, 2014).

[19] *See*, *e.g.*, Andrew Rens, *Collateral Damage: The Impact of ACTA and the Enforcement Agenda on the World's Poorest People*, 26 AM. U. INT'L L. REV. 783, 784–85 (2011) (arguing that there is no legitimate purpose "to enact national laws and create policies and practices which effectively eliminate existing limitations and exceptions in the current international intellectual property regime, at least with regard to cross border regulations of intellectual property").

[20] BUS. SOFTWARE ALLIANCE, SHADOW MARKET: 2011 BSA SOFTWARE PIRACY STUDY 4 (2012), *available at* http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

[21] *See*, *e.g.*, Robert G. Picard, *A Note on Economic Losses Due to Theft, Infringement, and Piracy of Protected Works*, 17 J. OF MED. ECON. 207, 209 (2004).

[22] U.S. INT'L TRADE COMM'N, http://www.usitc.gov/ (last visited Jan. 30, 2014).

[23] Peter K. Yu, *Enforcement, Enforcement, What Enforcement*?, 52 IDEA J. OF L. & TECH. 239, 245 (2012).

[24] BUS. SOFTWARE ALLIANCE, *supra* note 20, at 1.

[25] Stephen Ezell, *GAO Report on Economic Impact Underwhelms*, THE HILL'S CONG. BLOG (July 12, 2013, 6:00 PM), http://thehill.com/blogs/congress-blog/technology/310691-gao-report-on-economic-impact-from-ip-theft-underwhelms#ixzz2eLEf4odP.

[26] *Id.*

$4 billion in new economic activity and $660 million in additional tax revenue."[27] Nationally, a recent study highlights the negative impact that global software piracy has on U.S. manufacturers concerning jobs, revenue, and innovation.[28]

¶20 According to one commentator, "the average company lost $101.9 million in revenues and incurred costs of $1.4 million in identification and enforcement of intellectual property rights, leading to an average decline in profits of $46.3 million."[29] At least one source—U.S. Customs and Border Protection—has a precise way to describe the phenomenon: "[In 2011, it] seized 24,792 counterfeit or pirated goods, a 24.2 percent increase over the amount of goods seized in 2010.[30] These seized goods represented more than $1.1 billion in lost sales."[31]

¶21 According to a U.S. Department of Commerce report, the vast majority of the U.S. economy relies on IP in some form.[32] Of 313 total industries accounted for by the study, 75 are IP-intensive and account for 27.1 million American jobs (18.8 percent of all employment in the U.S. economy in 2010).[33] In 2010, IP-intensive industries comprised 34.8 percent of U.S. GDP (around $5.06 trillion in value added).[34] Furthermore, 60.7 percent of all U.S. merchandise exports came from IP-intensive industries.[35]

¶22 Andrew Hupert of Best Practices China, a consulting firm, maintains a website to help westerners negotiate more successfully in mainland China through a compilation of interactive online resources.[36] Hupert notes that while IP theft is declining in China, "IP theft is still the rule rather than the exception."[37] The risk is continuous. Hupert warns: "Westerners considering doing business in China have to plan on someone making a play for [their] IP. It's not a matter of 'if,' but 'when'—and 'who.' If your technology is any good, someone in your China supply chain is going to try to access it . . . if someone doesn't try to steal your designs and ideas, then something is wrong with your product or process."[38]

---

[27] *Calif. Workers Lose Billions in Wages Due to IT Piracy*, PR NEWSWIRE (Jan. 25, 2012), http://www.prnewswire.com/news-releases/report-calif-workers-lose-billions-in-wages-due-to-it-piracy-138063268.html.

[28] WILLIAM KERR & CHAD MOUTRAY, ECONOMIC IMPACT OF GLOBAL SOFTWARE THEFT ON U.S. MANUFACTURING COMPETITIVENESS AND INNOVATION 4 (2014) ("We estimate that reducing the global software piracy rate by 2.5 percentage points per year for 4 years would create 27,239 new manufacturing jobs, add $8.7 billion dollars to U.S. GDP, and generate $29.0 billion in revenue to manufacturers.").

[29] STAFF OF CHAIRMAN OF JOINT ECON. COMM., 112TH CONG., THE IMPACT OF INTELLECTUAL PROPERTY THEFT ON THE ECONOMY 2 (Comm. Print 2012), *available at* http://www.jec.senate.gov/public/index.cfm?a=Files.Serve&File_id=aa0183d4-8ad9-488f-9e38-7150a3bb62be.

[30] *Id.*

[31] *Id.*; *See* OFFICE OF INT'L TRADE, INTELLECTUAL PROPERTY RIGHTS FISCAL YEAR 2011 SEIZURE STATISTICS (2011), *available at* http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf; *Policy Feature Issue: Global Intellectual Property Theft*, HOUSE REPUBLICANS (June 4, 2013), http://www.gop.gov/blog/13/06/04/policy-feature-issue-global-intellectual-property-theft.

[32] STAFF OF CHAIRMAN OF JOINT ECON. COMM., *supra* note 29.

[33] IP COMMISSION REPORT, *supra* note 5, at 11.

[34] *Id.*

[35] *Id.*

[36] *See* Andrew Hupert, *IP Theft in China—Cost of Doing Business or Barrier to Entry*, CHINESENEGOTIATION.COM (Aug. 24, 2012), http://www.chinesenegotiation.com/2012/08/ip-theft-in-china-cost-of-doing-business-or-barrier-to-entry/.

[37] *See id*.

[38] *See id*.

¶23 Without reliable IP and IT protection, it is questionable whether the United States, or any country, could sustain the essential incentives for creativity, invention, and efficiency. As global theft of IT and IP through the supply chain increases, "American software developers are discouraged from investing in new technology and products when they know their software will be stolen."[39] This affects both inventors and investors. "IP theft's most insidious impact lies in undermining both the incentives and means to invest in innovative activity."[40] Viewed alone, no one enforcement regime can solve the problem. Viewed collectively, and operating in a coordinated manner, the complete array of domestic and international efforts, both public and private, can begin to turn the tide.

¶24 One final point on the impact of IP and IT theft requires no documentation: theft costs money. However you assess the problem, stolen IP and IT, viewed globally, has a price tag that runs into the trillions of dollars. A sustained, coordinated global campaign by public and private actors, as suggested in this Article, resulting in public support for criminal prosecution, civil enforcement, regulatory sanctions, and most importantly, a transnational cultural shift in public understanding of the hazards of IP and IT theft should bring down the cost of piracy. That gives rise to two highly desirable outcomes: more resources and thus motivation for innovation, creativity, and invention, and reduced prices for goods and services.

¶25 Common and necessary products that consist predominantly of IP and IT[41] carry a fairly high price tag.[42] High prices on essential items provide powerful motivation for theft.[43] It stands to reason that lower prices will decrease that motivation and the prevalence of theft.

¶26 The cost of theft is incorporated into the price of all predominantly IT- and IP-based products. Greatly reduce or eliminate the theft, and the theft-driven cost component diminishes. While it could be that reduced theft, and correspondingly, reduced theft costs, will translate solely into greater net profit, that is an inefficient outcome. If prices stay high, a powerful incentive for theft remains.[44] Thus, it is not in a producer's financial interest to maintain that theft incentive. Over time, significant reductions in theft should produce concomitant reductions in price, leading to less motivation for theft, stabilized profitability, and renewed incentives for invention and innovation.

---

[39] McKenna, *supra* note 14.

[40] Ezell, *supra* note 17.

[41] For example, essential software including programs for word-processing, e-communication, accounting, management, information gathering and organization, and other common uses, or hardware such as laptop computers or any form of e-pad—made by any legitimate producer.

[42] There are thousands of websites that discuss the high cost of IP- and IT-dominant software and hardware. Use any search engine with "high cost of software and computer hardware" and take your pick. Google reports about 66,700,000 results with this search. GOOGLE, https://www.google.com/ (last searched Sept. 6, 2014). There are likewise innumerable sites that explain in simple terms how to steal software. This author chooses not to provide a roadmap or instructional website on how to achieve the objective this Article seeks to prevent.

[43] *See* Joseph C. Nunes et al., *Why Are People So Prone to Steal Software? The Effect of Cost Structure on Consumer Purchase and Payment Intentions,* 23 J. PUB. POL'Y & MARKETING 43, 43 (2004), *available at* http://faculty.chicagobooth.edu/christopher.hsee/vita/Papers/WhyArePeopleSoProne.pdf.

[44] *Id*.

C. The Nature of Theft in the Supply Chain

¶27 U.S. companies operate internationally through trans-boundary supply chains and an increasingly globalized workforce supported by international capital markets.[45] The multinational nature of business increases the probability of "inadvertent, accidental or willful disclosure of confidential information and trade secrets."[46] When IP theft takes place beyond U.S. borders, there is limited recourse in domestic courts stemming, in part, from the difficulties associated with securing in personam jurisdiction over foreign defendants and the problem of enforcing domestic judgments outside the United States.[47]

¶28 Beyond jurisdictional problems, the stark reality exists that IP and IT theft within and surrounding international supply chains occurs in numerous forms, some of which are extraordinarily difficult to track. Certain types of IP theft are apparent, undertaken by employees at a very tactile or personal level. "Hard drives are either duplicated on site or physically stolen by bribed employees [and] employees are planted temporarily in companies or permanent employees leave and illegally share proprietary information . . . ."[48]

¶29 Other types of IP theft, while equally pernicious, are more difficult to track. "[P]roducts are dissected, re-engineered [and the original is returned intact] . . . . [The counterfeit product is then] sold without permission or payment of royalties [and] digitized products are pirated and sold illegally . . . ."[49] Another variety of IP theft involves misconduct by third parties not part of the direct line of production: "[P]hones are tapped for the purpose of obtaining trade secrets; and email accounts are compromised."[50] The IP Commission Report[51] mentions the different types of IP theft across sectors and the difficulties of measuring that theft.[52] Certain localized thefts are nearly invisible to the rights holder since the end-product reaching the United States does not reveal the misconduct, i.e., the product imported is not diminished yet the property of the inventor has been appropriated.

¶30 IP and IT theft is also seen as private-sector counterfeiting. The U.S. Department of Commerce includes in its definition of counterfeiting: electronics products that are unauthorized copies, which do not conform with the original component manufacturer

---

[45] David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1110–11 (2012).

[46] DONNA GHELFI, WORLD INTELLECTUAL PROP. ORG., THE 'OUTSOURCING OFFSHORE' CONUNDRUM: AN INTELLECTUAL PROPERTY PERSPECTIVE 8 (2005), *available at* http://www.wipo.int/export/sites/www/sme/en/documents/pdf/outsourcing.pdf.

[47] *See* Christopher L. Blakesley & Dan E. Stigall, *The Myopia of* U.S. v. Martinelli*: Extraterritorial Jurisdiction in the 21st Century*, 39 GEO. WASH. INT'L L. REV. 1, 3 (2007). *See generally* Andrew F. Popper, *Beneficiaries of Misconduct: A Direct Approach to IP Theft*, 17 MARQ. INTELL. PROP. L. REV. 27 (2013); Andrew F. Popper, *In Personam and Beyond the Grasp: In Search of Jurisdiction and Accountability for Foreign Defendants*, 63 CATH. U. L. REV. 155 (2013).

[48] IP COMMISSION REPORT, *supra* note 5, at 11.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See* RONALD KIRK, OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2012 SPECIAL 301 REPORT (2012), *available at* http://www.ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf; DEMETRIOS MARANTIS, OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2013 SPECIAL 301 REPORT (2013), *available at* http://www.ustr.gov/sites/default/files/05012013 percent202013 percent20Special percent20301 percent20Report.pdf.

(OCM), are not produced by the OCM, are off-specification or defective yet sold as new, or have false markings or documentation.[53] This definition includes pharmaceuticals and even "government[al] . . . weather communication system[s],"[54] and further suggests that counterfeiting information technology can endanger consumer safety and national security.[55]

¶31 Counterfeiting occurs with both entire product lines and component parts of end products. Risks regarding stolen IP and IT run the expanse of the supply chain, from raw materials to final product, compounding the difficulties of controlling or reducing theft.[56]

¶32 While one might think of IT and IP theft as a set of corporate decisions made by third-world multinationals determined to pirate and exploit the IT and IP of others, the actual thieves do not always fit that description. John Dowdy[57] presents a different image of IP and IT pirates. They are often young, twice as likely to live in an emerging economy as in a mature economy (38 percent as opposed to 15 percent),[58] and "install nearly four times as many programs of all sorts per new [personal computer] as do frequent pirates in mature markets."[59] Given that profile (younger and tech-savvy), it is worth asking what mechanisms would dissuade IP and IT theft. Would a U.S. enforcement action change the mind of a person who lives in an emerging economy and profits greatly from such theft? Would a U.S. enforcement action deter a tech-savvy IP thief in the developing world who needs but cannot afford access to expensive products that are dependent on or consist primarily of IP or IT?

¶33 This becomes a particularly challenging question in light of the belief structure or attitudes of those who want or need to make use of the IP or IT of another, but do not want to (or cannot) pay for it. As one commentator noted, "There's no social stigma attached to being a downloader the way that there is to, say, shoplifting . . . . [Even those] generally opposed to [unlawful] downloading . . . don't think of downloaders as morally repugnant people."[60] This problematic belief structure plays a powerful role in coming to grips with this issue.

¶34 In order to have a shot at reframing the belief structure of those described above, massive and sustained public information and educational programs should be initiated at the global level if there is to be some hope of influencing such behavior. Second, there ought to be a public and sustained across-the-board buy-in by governments of the basic

---

[53] U.S. DEP'T OF COMMERCE, DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS 212 (2010), *available at* http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010.

[54] Daniel Baldwin, Assistant Comm'r, U.S. Customs & Border Protection, Speech to the International Law Enforcement IP Crime Conference (June 26, 2008).

[55] *See* CTR. FOR RESPONSIBLE ENTER. & TRADE, HEALTH AND SAFETY RISKS FROM COUNTERFEITS IN THE SUPPLY CHAIN (2012) [hereinafter CTR. FOR RESPONSIBLE ENTER. & TRADE, HEALTH AND SAFETY RISKS].

[56] *See* CTR. FOR RESPONSIBLE ENTER. & TRADE, IP THEFT, *supra* note 8.

[57] John Dowdy is an IP commentator and director at McKinsey & Company. MCKINSEY & CO., http://www.mckinsey.com/client_service/aerospace_and_defense/people/john_dowdy (last visited Sept. 6, 2014).

[58] BUS. SOFTWARE ALLIANCE, *supra* note 20, at 1.

[59] *Id.* at 2.

[60] Brian Spears, *Missing the Point on Content Piracy*, THE RUMPUS (Jan. 28, 2012), http://therumpus.net/2012/01/missing-the-point-on-content-piracy/; *see* Peter Lewin, *Creativity or Coercion: Alternative Perspectives on Rights to Intellectual Property*, 71 J. BUS. ETHICS 441, 445 (2007).

premise that theft of IP and IT is a wrongful act with significant and far-reaching negative consequences.[61]

¶35 As the materials that follow demonstrate, within the United States, there are ongoing prosecutions and public-information campaigns, as well as a presidential commission, all focused on IP and IT theft. Some of these efforts as well as some broad-based international initiatives follow.

III. Domestic and International Efforts to Address Theft in the Supply Chain

¶36 In 2012, the Business Software Alliance (BSA) issued a report detailing tens of billions of dollars annually in lost value within the United States as a consequence of stolen IP and IT "driven primarily by theft in emerging market economies such as China, Russia, India, and Brazil."[62] For U.S. businesses, "this is like trying to compete when two-thirds of your competitors do not have to pay for basic costs of doing business, like rent or utilities."[63] Finding a solution to stolen IP and IT is hard enough. Finding a solution when the primary actors causing harm in the United States are outside the country makes this a far more challenging problem.

¶37 When foreign entities are involved, the most basic approach to prevention is § 337 of the Tariff Act of 1930, allowing either the ITC or an injured party to pursue sanctions including a ban on those products made with stolen or infringed IP and IT.[64] Section 337 has been interpreted as applicable to misappropriation of trade secrets occurring outside the United States when the products produced through the misappropriation are imported to the United States.[65] In 2011, the ITC published a report on the need for and uses of this section, though to date there has been no meaningful follow-up.[66] Moreover, the explosion in IP and IT theft has taken place notwithstanding the enforcement option of § 337, suggesting the necessity for other approaches. As with every other sanction or remedy mentioned, § 337 is part of the solution, even though on its own it has not been, and will not be, the answer to the IP-theft problem.

¶38 Assuming one can secure jurisdiction, one approach is state common law claims. For example, unjust enrichment, like other unfair competition claims, could allow the use of "old laws . . . to address specific abuses of intellectual property rights that threaten

---

[61] While members of the WTO agree generally to this precept, there are significant qualifiers. The World Trade Organization implementation of this "pledge" is in TRIPS. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS]. "Members shall ensure that enforcement procedures as specified in this Part are available under their law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements." *Id.* art. 41. Articles 65 and 66 extend the time frame for compliance as long as ten years for developing countries that do not have in place any semblance of an IP-protecting legal system. *Id.* art. 65–66.

[62] David J. Kappos & Gregory R. Baden, *Combating IP Theft Using Unfair Competition Law*, N.Y.L.J. (May 6, 2013), *available at* http://www.cravath.com/files/Uploads/Documents/Publications/3409818_1.pdf.

[63] *Id.*

[64] 19 U.S.C. § 1337 (2006).

[65] TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1332 (Fed. Cir. 2011).

[66] China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, Inv. No. 332-519, USITC Pub. 4226 (May 2011) (Final).

competition in the market."[67] University of Pennsylvania legal scholar, Professor Shyamkrishna Balganesh, observed, "[T]here exists a rather robust body of state law that is almost entirely the creation of state courts and is directed at creating entitlements in information, ideas, expression, goodwill, one's image, and other related intangibles. These rights regimes are in turn collectively referred to as 'common law intellectual property.'"[68]

¶39 It is essential to make sure there is public awareness of both the IP- and IT-theft problem and the legal enforcement proceedings thereof. For example, Mississippi's Intellectual Property Crime Center, an entity designed to inform citizens of the dangers of IP theft, and how to identify and report violations thereof, illustrates this objective.[69] Centers or other organizations of this nature can play an important role not only in identifying IP theft, but also in sponsoring and promoting the marketing, educational, and advertising programs needed for the critical cultural change—the across-the-board public understanding and rejection of IT theft.

¶40 Beyond public education, there is an essential role for state civil and criminal enforcement. State laws typically emphasize an unfair trade or unfair competition approach with "state attorneys general . . . using the tools of unfair competition law in an attempt to level the playing field for American competitors."[70] State statutes often provide a broader definitional standard for unfair competition than federal law,[71] and in some states can "provide for a private right of action [for] misappropriated IT."[72]

¶41 Fourteen states have adopted or are considering new statutes that address unauthorized use of IT.[73] These statutes can push beyond substantive limitations of common law claims to get at varying aspects of the theft of IT and IP. For example, Washington's unfair competition statute[74] does not require the incorporation of the stolen IT or IP into the product sold in the state:

> [I]t is sufficient for liability . . . if the IT is used in business operations (such as distribution, sales and marketing, inventory, logistics and accounting). Thus a supplier's illegal use of software in its business

[67] Emilio Varanini, *The Use of Unfair Competition Laws to Address Intellectual Property Practices that Injure Market Competition*, 2013 A.B.A. SEC. ANTITRUST L. 8, *available at* http://www.americanbar.org/content/dam/aba/publications/antitrust_law/20130626_at13626_materials.authcheckdam.pdf.

[68] Shyamkrishna Balganesh, *The Pragmatic Incrementalism of Common Law Intellectual Property*, 63 VAND. L. REV. 1543, 1544 (2010).

[69] *See* MISS. INTELLECTUAL PROP. CRIME CTR., http://mipcc.ago.state.ms.us/DidYouKnow.aspx (last visited Sept. 6, 2014).

[70] Kappos, *supra* note 62.

[71] *See* Varanini, *supra* note 67.

[72] Kappos, *supra* note 62.

[73] These states are Arizona, California, Connecticut, Illinois, Indiana, Kentucky, Louisiana, Massachusetts, Missouri, New York, North Carolina, Oregon, Utah, and Washington. *See* ARTHUR M. MITCHELL III ET AL., WHITE & CASE, THE EMERGING RISKS OF UNAUTHORIZED IP IN YOUR SUPPLY CHAIN AND HOW YOU SHOULD RESPOND 8–9 (2013); Daniel Shickich, *Finding Safe Harbor: Navigating Washington's New Unfair Competition Law*, 8 WASH. J.L. TECH. & ARTS 1, n.19 (2012) (enumerating those states that have considered but not passed legislation designed to facilitate prosecution of IP and IT theft).

[74] WASH. REV. CODE § 19.330.020 (2011).

> operations would put the supplier—and potentially the company that relies on that supplier in its supply chain—squarely in the law's crosshairs.[75]

¶42 While a number of states have taken aim at IT and IP theft,[76] the scope of the global problem is far too great to expect that isolated state enforcement will be sufficient. Nonetheless, the states' actions are a critical and impressive step forward. "With little apparent help on the horizon from federal officials, concerted efforts by business and state attorneys general could prove a strong weapon to claw back some of the billions of dollars in ill-gotten advantage foreign companies are enjoying . . . ."[77]

¶43 Both Massachusetts[78] and California[79] have prosecuted IT and IP thefts using similarly broad laws to hold companies and their global suppliers accountable.[80] Tennessee has also taken an aggressive and positive role enforcing its unfair competition law, and recently initiated a case against an overseas manufacturer using stolen IP.[81] A Washington case, brought against the Brazilian airplane-manufacturing giant Embraer using the aforementioned Washington statute,[82] was recently settled, indicating the power of state laws to influence behavior outside the United States.[83] These state cases give hope to victims of IT and IP theft, but cannot resolve certain overt roadblocks to enforcement. First, federal law occasionally still preempts potential actions under state law.[84] Second, the jurisdictional problems associated with domestic enforcement are considerable.[85] Third, the remedial potential of state cases is limited, particularly when one of the key actors involved in the theft resides outside the United States.

---

[75] MITCHELL III ET AL., *supra* note 73, at 9.

[76] As discussed *supra* note 73, prosecution of IT or IP theft has gone forward in California, Illinois, Kentucky, Massachusetts, New Jersey, New York, Utah, Washington, and Wisconsin.

[77] Kappos, *supra* note 62.

[78] Assurance of Discontinuance Pursuant to G.L. c. 93A, § 5 ¶ 5, Commonwealth v. Narong Seafood Co., No. 12-3825A (Mass. Dist. Ct. 2012) (discussing prosecution and imposition of fines on Narong, a Thailand-based seafood processer); *see* Press Release, Att'y Gen. of Mass., Company Fined for Using Pirated Software to Gain Unfair Advantage over Massachusetts Business (Oct. 18, 2012), *available at* http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-10-18-narong-seafood-co.html.

[79] Press Release, Office of the Att'y Gen., Cal. Dep't of Justice, Attorney General Kamala D. Harris Files Unfair Competition Lawsuits over Use of Pirated Software in Apparel Industry (Jan. 24, 2013), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-unfair-competition-lawsuits-over-use.

[80] MITCHELL III ET AL., *supra* note 73, at 10.

[81] *See State AGs Developing Groundbreaking Solutions to Battle IT Theft and Unfair Competition, ABA Panelists Report*, WALL ST. J. (June 26, 2013), http://online.wsj.com/article/PR-CO-20130626-909922.html.

[82] WASH. REV. CODE § 19.330.020 (2011).

[83] *See* Press Release, Wash. State Office of the Att'y Gen., Washington's New Unfair Competition Law Protects Local Company from Software Piracy (Apr. 3, 2013), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=31143#.UmvisV_D-T8.

[84] *See* TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1325 (Fed. Cir. 2011) ("The question of what law applies in a section 337 proceeding involving trade secrets is a matter of first impression for this court. We hold that a single federal standard, rather than the law of a particular state, should determine what constitutes a misappropriation of trade secrets sufficient to establish an 'unfair method of competition' under section 337.").

[85] *See generally* Andrew F. Popper, *Beneficiaries of Misconduct: A Direct Approach to IP Theft*, 17 MARQ. INTELL. PROP. L. REV. 27 (2013) (discussing issues with domestic enforcement); Andrew F. Popper, *In Personam and Beyond the Grasp: In Search of Jurisdiction and Accountability for Foreign Defendants*, 63 CATH. U. L. REV. 155 (2013) (discussing jurisdictional issues).

A. A Sampling of State Cases

¶44 Many IP and IT theft cases and most trade secret cases are adjudicated in state courts.[86] Since a number of state laws provide opportunities to address different types of IT or IP theft,[87] it is worth looking at some examples of what different states have done to deal with the problem.

1. California

¶45 California recently filed suit[88] against two apparel manufacturers for using pirated software.[89] The defendants, one Chinese and one Indian, allegedly used software without paying the licensing fees, which gave them a "substantial and unfair" cost advantage over their competitors in California.[90] In announcing the prosecution, State Attorney General Kamala Harris blamed IP and IT piracy for the loss of "nearly 400,000 manufacturing and technology jobs over the past decade to countries where piracy rates are as high as 80 percent."[91]

¶46 In a recent setback for California, an international defendant's motion to quash service of process was granted.[92] This case illustrates both a state's resolve to address IP and IT theft and the common problems associated with litigating against foreign defendants. The case centers on Pangang Group, "a state-owned enterprise of the People's Republic of China[], controlled by the State-Owned Assets Supervision and Administration Commission of the State Council."[93] California state agents, unable to serve process on Pangang in China, served an office manager of a company doing business in the United States for Pangang and sent four copies of the summons via certified mail to Pangang's New Jersey office.[94]

¶47 Pangang moved to quash service of process pursuant to Federal Rule of Criminal Procedure 4(c).[95] Rule 4(c)(2) allows a "summons [to] be served 'within the jurisdiction of the United States or anywhere else a federal statute authorizes an arrest.'"[96] The court pointed out that service of process in a criminal case requires personal service of

---

[86] *See* Leggett & Platt v. Hickory Springs Mfg., 285 F.3d 1353, 1360 (Fed. Cir. 2002) (addressing trade secret misappropriation of a patented bedding foundation based on the Illinois Trade Secrets Act); Group One, Ltd. v. Hallmark Cards Inc., 254 F.3d 1041, 1049–50 (Fed. Cir. 2001) (applying Missouri common law, since the Missouri trade secret law was inapplicable to acts occurring prior to 1995, to analyze trade secret misappropriation of a patented ribbon-curling method).

[87] McKenna, *supra* note 14. Requesting federal action, however, "need not preclude state enforcement of intellectual property protections, either." *Id.* "While states are a key battleground . . . we need a federal solution. Federal enforcement would elevate public awareness and provide a powerful national remedy to a problem that is clearly national in its impact and scope." *Id.*

[88] Press Release, Office of the Att'y Gen., Cal. Dep't of Justice, *supra* note 79.

[89] *Id.*

[90] MITCHELL III ET AL., *supra* note 73, at 9 (citing Complaint for Injunction and Civil Penalties, California v. Pratibha Syntex Ltd., No. BC499751 (Cal. Super. Ct. 2013); Complaint for Injunction and Civil Penalties, California v. Ningbo, No. BC499771 (Cal. Super. Ct. 2013)).

[91] Press Release, Office of the Att'y Gen., Cal. Dep't of Justice, *supra* note 79. Further, this has drained California of $1.6 billion in value and $700 million in lost taxes. *Id.*

[92] United States v. Pangang Group, 879 F. Supp. 2d 1052, 1055 (E.D. Cal. 2012).

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.* at 1057.

defendants or the defendants' "general agent."[97] To be the general agent, the court required the government to show that the party served in the United States was "the alter-ego"[98] of the defendant, something the government could not do. Accordingly, the court granted the defendants' motion and quashed service on the defendants.

¶48 The alter-ego requirement and other technical problems with this case will come up in IT and IP theft cases where there are independent domestic producers or sellers acting on behalf of foreign or nonresident defendants. For jurisdiction purposes, the domestic seller and the foreign entity ought to be seen as part of the single supply chain, thus facilitating service of process. Instead, the court found that since the target of the investigation was outside the United States and had insufficient minimum contacts in the United States, service on the domestic entity was not service on the foreign entity.[99] These jurisdictional issues are not easily resolved (if they can be resolved at all), and are present in many of the state-initiated cases.[100]

2. Illinois

¶49 In 2012, Chunlai Yang, a former employee of Chicago-based CME Group, pled guilty to "two counts of theft of trade secrets for stealing source code and other proprietary information while at the same time pursuing plans to improve an electronic trading exchange in China."[101] Yang, a senior software engineer,[102] admitted to downloading more than 10,000 of the company's files, including the source code for the Globex electronic trading platform.[103] It is estimated that the company lost up to $100 million as a result of the theft.[104] Yang stole the files by downloading them to flash drives and copying the files to his personal computers at home.[105] The defendant's purpose "was to increase the trading volume at the Zhangjiagang, China, chemical electronic trading

[97] *Id.* at 1052, 1058.
[98] *Id.* at 1066.
[99] *See* Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102, 113 (1987); Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 415–18 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 294 (1980); Hanson v. Denckla, 357 U.S. 235, 253 (1958); Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945) (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)); Joel R. Paul, *Comity in International Law*, 32 HARV. INT'L L.J. 1, 76–77 (1991).
[100] *See* Goodyear Dunlop Tires Operations, S.A. v. Brown, 131 S. Ct. 2846, 2851 (2011) (citations omitted) ("A court may assert general jurisdiction over foreign (sister-state or foreign-country) [defendants] when their affiliations with the State are so 'continuous and systematic' as to render them essentially at home in the forum State. Specific jurisdiction . . . depends on an 'affiliation between the forum and the underlying controversy,' principally, activity or an occurrence that takes place in the forum State. . . . [S]pecific jurisdiction is confined to adjudication of 'issues deriving from, or connected with, the very controversy that establishes jurisdiction.'"); J. McIntyre Machinery, Ltd. v. Nicastro, 131 S. Ct. 2780 (2011).
[101] DEP'T OF JUSTICE, SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES 1, 9–10 (2014); *see* Indictment at 6, United States v. Chunlai Yang, No. 11 CR 458 (N.D. Ill. 2011).
[102] DEP'T OF JUSTICE, *supra* note 101.
[103] *Id.*
[104] *Id.*
[105] *Id.*

exchange (the Zhangjiagang Exchange)."[106] Attempts to settle the case were ultimately successful,[107] and Yang will serve time in prison for this theft.[108]

3. Massachusetts

¶50 In 2012, Massachusetts initiated an action against a Thai seafood distributor, Narong, alleging theft of IP covered under the state's unfair competition law.[109] This was the first of the new wave of state-initiated IP or IT piracy/theft/misappropriation cases brought by a state attorney general.[110] Massachusetts alleged that Narong's failure to pay licensing fees for the software used to produce and sell its products was a violation of the state unfair competition law.[111] The attorney general noted that users of unlicensed software gain an unfair advantage over businesses that follow the rules.[112] The action resulted in an agreement in which "Narong . . . agreed not to illegally use unlicensed copyrighted software programs in connection with the production or manufacturing of goods that enter Massachusetts."[113] Narong will also pay a $10,000 civil penalty.[114]

4. New Jersey

¶51 *a) United States v. Maniar*.[115]—In June 2013, Epstein Becker Green, on behalf of Becton, Dickinson & Company (BD), filed a civil action in New Jersey against former BD employee, Ketankumar Maniar.[116] This lawsuit led to a restraining order against Maniar preventing him from leaving the country with trade secret information obtained from BD.[117] This action has drawn the attention of federal law enforcement after it was alleged that Maniar had developed a "tool-kit" to manufacture an unreleased, prefilled

---

[106] *Id.*

[107] *See* Plea Agreement, United States v. Chunlai Yang, No. 11 CR 458 (N.D. Ill. 2012), *available at* http://www.justice.gov/usao/iln/pr/chicago/2012/pr0919_01a.pdf.

[108] Andrew Harris, *Ex-CME Software Engineer Admits to Trade-Secrets Theft*, BLOOMBERG (Sept. 19, 2012, 3:40 PM), http://www.bloomberg.com/news/2012-09-19/ex-cme-group-software-engineer-admits-secrets-theft-u-s-says.html.

[109] Press Release, Att'y Gen. of Mass., *supra* note 78; *see* Assurance of Discontinuance Pursuant to G.L. c. 93A, §5 ¶ 5, Commonwealth v. Narong Seafood Co., No. 12-3825A (Mass. Dist. Ct. 2012); *see also* Michael B. Farrell, *Massachusetts Fines Thai Seafood Company over Pirated Software*, BOS. GLOBE (Oct. 19, 2012), http://bostonglobe.com/business/2012/10/18/massachusetts-fines-thai-seafood-company-over-pirated-software/ZdfHGXTTSVMzlI0pQLcnhP/story.html; Ira Kantor, *Thai Seafood Company to Pay $10G Penalty over Unfair Practices*, BOS. HERALD (Oct. 18, 2012), http://bostonherald.com/business/technology/technology_news/2012/10/thai_seafood_company_pay_10g_penalty_over_unfair; Patricia Resende, *State Fines Thai Company for Pirated Software Use*, BOS. BUS. J. (Oct. 18, 2012), http://www.masshightech.com/stories/2012/10/15/daily46-State-fines-Thai-company-for-pirated-software-use.html.

[110] *See* Farrell, *supra* note 109; *see also* Kantor, *supra* note 109; Resende, *supra* note 109.

[111] *See* Resende, *supra* note 109.

[112] *See* Press Release, Att'y Gen. of Mass., *supra* note 78.

[113] *Id*.

[114] *Id.*

[115] *Former Engineer at Two Global Medical Technology Corporations Admits Theft of Trade Secrets*, FED. BUREAU OF INVESTIGATION (May 28, 2014), http://www.fbi.gov/newark/press-releases/2014/former-engineer-at-two-global-medical-technology-corporations-admits-theft-of-trade-secrets.

[116] James P. Flynn, *Federal Trade Secret Enforcement Initiative Results in Swift Action*, LEXOLOGY (June 10, 2013), http://www.lexology.com/library/detail.aspx?g=5f38fab7-acd1-41c6-8f99-27f530835855.

[117] *Id.*

pen injector made by BD in contravention of the Economic Espionage Act (EEA).[118] Both the state civil action and federal criminal case are pending.[119]

¶52 *b) United States v. Liu*.—In March 2013, Sixing "Steve" Liu, a Chinese national, was sentenced to seventy months in prison for export control and other violations.[120] Liu's convictions were for violating the EEA, the International Traffic in Arms Regulations, and the Arms Export Control Act.[121] Liu stole thousands of electronic files from his New Jersey-based employer, the Space and Navigation Division of L-3 Communications Holdings, Inc.[122] This information included details about "the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles."[123] Liu took the stolen files to China and delivered presentations about the technology at several Chinese universities.[124] Liu used the stolen information to gain employment at a premier Chinese aeronautical institute.[125] The question of whether Liu will be required to pay restitution is pending.[126]

¶53 *c*) *United States v. Li*.—In January 2012, Yuan Li, a former research scientist for Sanofi Aventis, pled guilty to violating the EEA[127] and was sentenced to eighteen months in prison.[128] Li, a Chinese national, admitted to stealing data regarding chemical structures and sending that information via email or through use of a thumb drive.[129] Li was required to pay $131,000 to Sanofi as restitution.[130]

5. New York

¶54 *United States v. Agrawal*, decided in August 2013, affirmed a conviction for an EEA and a National Stolen Property Act (NSPA) violation against Samarth Agrawal, a former employee of the French bank, Societe Generale (SocGen).[131] Agrawal had access

---

[118] *Id.*; *see* Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2012).

[119] Flynn, *supra* note 116; *see Former Engineer for Global Medical Technology Corporation Charged with Stealing Trade Secrets from New Jersey Employer*, FED. BUREAU OF INVESTIGATION (June 5, 2013), http://www.fbi.gov/newark/press-releases/2013/former-engineer-for-global-medical-technology-corporation-charged-with-stealing-trade-secrets-from-new-jersey-employer.

[120] Eric Carlson et al., *Chinese National Sentenced to Nearly Six Years in Prison for Illegally Exporting U.S. Military Technology*, LEXOLOGY (Mar. 31, 2013), http://www.lexology.com/library/detail.aspx?g=69702201-3034-480a-83fc-cb172ed7fb72.

[121] *Id.*; *see* Verdict Form, United States v. Liu, No. 11-208, 2012 WL 4378706 (D.N.J. Sept. 26, 2012). *See generally* 22 U.S.C. § 2778 (2012); 18 U.S.C. §§ 1831–39 (2012); International Traffic in Arms Regulation, 22 C.F.R. §§ 120–30 (2013).

[122] Carlson et al., *supra* note 120; *see* Verdict Form, *supra* note 121. *See generally* 22 U.S.C. § 2778.

[123] Carlson et al., *supra* note 120; *see* Verdict Form, *supra* note 121.

[124] Carlson et al., *supra* note 120; *see* Verdict Form, *supra* note 121.

[125] Peter Finn, *Chinese Citizen Sentenced in Military Data-Theft Case*, WASH. POST (Mar. 25, 2013), http://articles.washingtonpost.com/2013-03-25/world/38006926_1_development-of-military-technologies-information-and-technologies-chinese-citizen.

[126] *Id.*

[127] Justin K. Beyer, *Trade Secret Theft Prosecution Cases in the News*, LEXOLOGY (May 16, 2012), http://www.lexology.com/library/detail.aspx?g=cd8f1d10-66b9-431c-bf25-5b6a9c2ed047; Press Release, Dist. of N. J., U.S. Att'y's Office, Former Research Chemist at Global Pharmaceutical Company Sentenced to 18 Months in Prison for Theft of Trade Secrets (May 7, 2012), *available at* http://www.justice.gov/usao/nj/Press/files/Li,%20Yuan%20Sentencing%20News%20Release.html.

[128] Beyer, *supra* note 127.

[129] *Id.*

[130] *Id.*

[131] United States v. Agrawal, 726 F.3d 235, 237 (2d Cir. 2013).

to confidential computer codes used to conduct securities trades.[132] Agrawal printed these codes and took them to his home in New Jersey to copy SocGen's trading system for a competitor.[133] The issue on appeal was not whether Agrawal was a thief, but whether he was properly convicted under the EEA and NSPA.[134]

¶55 Agrawal argued that in light of the recent decision in *United States v. Aleynikov*,[135] the government had to show that the stolen codes were "included in SocGen's HFT systems . . . [and] produced for or placed in interstate or foreign commerce as required by the EEA."[136] Although it was arguable that the codes were "valuable only in relation to the securities whose interstate trades it facilitated,"[137] the government met the "produced for or placed in interstate or foreign commerce" requirement and the conviction was affirmed.[138]

6. Utah

¶56 In 2012, a chemist from Frontier Scientist Inc., pled guilty to "one count of unlawful access to a protected computer."[139] The defendant unlawfully accessed Frontier Scientist Inc.'s chemical-resource notebook and emailed information regarding chemical formulas to his brother-in-law, who lived in India.[140] On review, however, the court dismissed the case.[141] The judge determined that the "'secret' chemical recipe was not only widely known to professionals in the field, but inferior in some respects."[142] The court held that the defendant had served an appropriate amount of time, thirty days, for the unlawful use of the company's computers.[143]

7. Virginia

¶57 One of the more recent cases in this field involves Kolon Industries.[144] Kolon, a South Korean company, was indicted in Virginia for allegedly attempting to steal trade secrets regarding DuPont's Kevlar para-aramid fiber.[145] The indictment sought at least $225 million from the trade secret theft.[146] Kolon produces Heracon, similar to Kevlar

---

[132] *Id.* at 238.
[133] *Id.* at 239.
[134] *Id.* at 237.
[135] United States v. Aleynikov, 676 F.3d 71, 73 (2d Cir. 2012) (reversing EEA and NSPA convictions on grounds of legal insufficiency when the government failed to demonstrate that the stolen IP was "produced for or placed in interstate or foreign commerce").
[136] *Agrawal*, 726 F.3d at 242 (citations omitted).
[137] *Id.* at 248.
[138] *Id.* at 262.
[139] Beyer, *supra* note 127.
[140] *Id.*
[141] Paul Foy, *Trade-Theft Case Collapses in Federal Court*, BLOOMBERG BUSINESSWEEK (June 5, 2013), http://www.businessweek.com/ap/2013-06-05/trade-theft-case-collapses-in-federal-court.
[142] *Id.*
[143] *Id.*
[144] United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794 (E.D. Va. 2013).
[145] Indictment at 1, 10, *Kolon Indus.*, 926 F. Supp. 2d 794 (No. 3:12-CR-137), *available at* http://tsi.brooklaw.edu/sites/tsi.brooklaw.edu/files/filings/united-states-v-kolon-industries-inc-et-al/20120821kolon-indictment.pdf.
[146] *Id.* at 35.

and Twaron, which are products used to make body armor and fiber-optic cables.[147] Kevlar is made by DuPont.[148] According to the indictment, Kolon hired current and former DuPont employees to assist with the theft.[149]

¶58 Kolon argued that since this is a criminal case, the United States must serve personally either Kolon or an appropriate U.S. agent. The government attempted service through MLAT (Mutual Legal Assistance Treaty).[150] Kolon countered that the MLAT simply does not encompass the procedure for securing service of process abroad in this case.[151] The government claimed it had taken the steps necessary to perfect service of "process pursuant to the U.S.-Korea MLAT."[152] The case is fairly typical of enforcement actions involving foreign defendants (not domiciled in the United States).[153] It is also indicative of the limitations on state enforcement in IP- and IT-theft cases.[154] Like *Panang*, *Kolon* shows the substantial problems regarding jurisdiction and remedies.

¶59 Separate from the indictment, DuPont successfully sued Kolon and won a $919 million judgment.[155] In August 2013, DuPont sought judicial assistance to enforce the judgment in New York and lost. The court found that in this instance Kolon was beyond its jurisdictional reach,[156] highlighting again the difficulties victims of IP theft face in securing relief, even after winning a judgment on the merits.

8. Washington

¶60 Washington has been at the forefront of state efforts to prosecute IT and IP theft as unfair competition. In 2011, the state adopted a broad-ranging law "aimed at giving domestic businesses a remedy against overseas IP infringement."[157] "[The law] creates a new cause of action allowing private plaintiffs or the state attorney general to seek damages and injunctive relief against a manufacturer of products sold in

---

[147] *Id.* at 3.

[148] *Better, Stronger and Safer with Kevlar Fiber*, DUPONT, http://www.dupont.com/products-and-services/fabrics-fibers-nonwovens/fibers/brands/kevlar.html (last visited Sept. 6, 2014).

[149] Indictment at 8, *Kolon Indus.*, 926 F. Supp. 2d 794 (No. 3:12-CR-137).

[150] *See generally* Mut. Legal Assistance Treaty, U.S.-U.K., Jan. 6, 1994, T.I.A.S. No. 96-1202, *available at* http://www.state.gov/documents/organization/176269.pdf.

[151] *Kolon Indus.*, 926 F. Supp. 2d at 817–18; *see* D.I. 37-1 at 8 (MLAT, Art. I § 3).

[152] Response in Opposition to Specially-Appearing Defendant Kolon Industries, Inc.'s Motion to Quash Service and to Dismiss the Superseding Indictment at 9, *Kolon Indus.*, 926 F. Supp. 2d 794 (No. 3:12-CR-137).

[153] *Kolon Succeeds in Getting Its Trade Secret Theft Arraignment Postponed*, SULLIVAN TRADE SECRETS (June 7, 2013), http://sullivantradesecrets.com/kolon-succeeds-in-getting-its-trade-secret-theft-indictment-postponed/.

[154] *E.I. DuPont de Nemours & Co. v. Kolon Industries, Inc.* preceded the 2013 *Kolon* criminal proceeding (still underway). 894 F. Supp. 2d 691 (E.D. Va. 2012). In that 2012 civil case between DuPont and Kolon, DuPont sued Kolon, alleging that there was misappropriation of trade secrets, and Kolon counterclaimed, accusing DuPont of monopolization or attempting to monopolize the para-aramid fiber market. *Id.* at 691. The antitrust claim was dismissed for "failure to sufficiently plead a relevant geographical market." *Id.* After the court of appeals reversed that decision, and after a jury trial on the merits, Kolon was found liable pursuant to the Virginia Uniform Trade Secrets Act. *Id.* DuPont requested and was granted a permanent injunction. *Id.* at 694.

[155] E.I. DuPont de Nemours & Co. v. Kolon Indus., No. 3:09cv58, 2011 U.S. Dist. LEXIS 134821, at *3 (E.D. Va. Nov. 22, 2011).

[156] E.I. DuPont de Nemours & Co. v. Kolon Indus., 12 Civ. 8435 (AJN), 2013 U.S. Dist. LEXIS 123949, at *2 (S.D.N.Y. Aug. 29, 2013).

[157] Shickich, *supra* note 73, at 3; *see* WASH. REV. CODE § 19.330.020 (2011).

Washington . . . ."[158] While this offers businesses a way to protect their IP and IT, it does not resolve the challenges extant in cases against foreign companies. "Lax IP protections abroad result in limited legal remedies for IT license holders in the United States."[159] The presence of the law suggests that "it is possible that . . . foreign manufacturers will begin to bring their IT into compliance."[160] However, "it is also possible that some manufacturers will find alternatives to avoid prosecution, such as creating separate reselling companies to sell into the Washington market."[161]

¶61 Washington's unfair competition law recently prompted the settlement of an IP theft claim asserted by Microsoft against Embraer; a foreign aircraft manufacturer that was allegedly misappropriating U.S.-owned and -protected software.[162] The Embraer settlement represents the merger of public and private resources at the state level to secure protection of IP because the Washington State Attorney General worked with Embraer to bring its business practices into compliance with state law. The Office of the State Attorney General noted this was an effective use of the "state's new unfair competition law to resolve a dispute over software licensing issues. . . . [The State] exchanged several letters with Embraer, the Brazilian company at the center of the dispute, in an effort to resolve the matter before taking more formal steps."[163] Sharing the steps taken to achieve this success and publishing widely the facts of the settlement would be of great value in the quest to mitigate IP and IT theft. A global partnership committed to this goal could achieve that objective far more easily than a state attorney general.

9. Wisconsin

¶62 In June 2013, a federal grand jury in Wisconsin indicted three individuals and Sinovel, Inc., a manufacturer and exporter of wind turbines in the People's Republic of China, for "conspiracy to commit trade secret theft, theft of trade secrets, and wire fraud."[164] The indictment accused the defendants of "stealing technology from American Superconductor Corp. of Devens (AMSC)."[165] Further, it noted that the defendants used stolen software taken from AMSC to make four of Sinovel's wind turbines.[166] The

[158] Shickich, *supra* note 73, at 3.
[159] *Id.* at 1, 6.
[160] *Id.* at 1, 26.
[161] *Id.*
[162] Press Release, Wash. State Office of the Att'y Gen., Washington's New Unfair Competition Law Protects Local Company from Software Piracy (Apr. 3, 2013), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=31143#.UmvisV_D-T8.
[163] Jessica M. Karmasek, *Wash. AG: State's New Unfair Competition Law Put to Use*, LEGAL NEWSLINE (Apr. 4, 2013, 8:00 AM), http://legalnewsline.com/news/240591-wash-ag-states-new-unfair-competition-law-put-to-use (pitting Microsoft against "Embraer, the world's fourth largest aircraft manufacturer, [which] produces commercial, military and executive aircraft and provides other aeronautical services").
[164] *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets*, DEP'T OF JUSTICE (June 27, 2013), http://www.justice.gov/opa/pr/2013/June/13-crm-730.html.
[165] Erin Ailworth, *Theft Case Against Chinese Firm Carries a Warning*, BOS. GLOBE (June 30, 2013), http://www.bostonglobe.com/business/2013/06/29/sinovel-case-could-protect-technology/SJzQJI96mTYwOH7LH9Ey2J/story.html; *see also* United States v. Sinovel Wind Grp. Co., No. 13-cr-00084 (W.D. Wis. 2013); Michael Riley, *China's Sinovel Charged with Stealing Trade Secrets*, BLOOMBERG (June 27, 2013), http://www.bloomberg.com/news/2013-06-27/china-s-sinovel-charged-with-stealing-trade-secrets.html.
[166] Riley, *supra* note 165.

indictment also alleged that the defendants conspired to steal trade secrets and cheated AMSC out of more than $800 million.[167] Sinovel also allegedly recruited an employee to leave AMSC, join Sinovel, and bring secretly copied IP from AMSC to Sinovel.[168] AMSC previously attempted to file suit against Sinovel in China, but Sinovel appealed those cases and the parties are awaiting resolution.[169] Among the arguments in the case is the same "alter-ego" problem noted earlier in the California *Pangang* case.[170]

B. Jurisdictional Challenges with Cybercrime

¶63 The Department of Justice defines computer crimes as "any violation[] of criminal law that involve[s] a knowledge of computer technology for their perpetration, investigation, or prosecution."[171] The Department's prosecution manual notes that while many statutes were created to impose punishment for domestic cybercrimes and to extend beyond U.S. borders, the statute must provide an "interstate or foreign jurisdictional hook."[172] The presence of the Internet alone could arguably satisfy this requirement due to its "inexorable connection" with interstate commerce,[173] but that does not resolve the problems associated with securing personal jurisdiction over foreign defendants.

¶64 Most U.S. criminal laws do not have extraterritorial jurisdiction absent clear congressional intent.[174] Importantly for IT and IP, domestic patent and copyright laws typically do not apply extraterritorially.[175] Trademark protection under the Lanham Act[176] pertaining to extraterritorial misconduct by foreign defendants is possible only when conduct "has a substantial effect on United States commerce by way of importing goods into the United States."[177] Even if misconduct is found, foreign defendants may argue they are not subject to the lawsuit in that forum and seek dismissal based on forum non conveniens.[178] And generally, no matter what statute is used to pursue trans-boundary IP or IT theft, extraterritorial application must be clear based on the plain meaning of the

---

[167] *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets*, DEP'T OF JUSTICE (June 27, 2013), http://www.justice.gov/opa/pr/2013/June/13-crm-730.html.

[168] *Id.*

[169] Ailworth, *supra* note 165.

[170] *See supra* notes 93–98 and accompanying text.

[171] Eric J. Bakewell et al., *Computer Crimes*, 38 AM. CRIM. L. REV. 481, 483 (2001) (citing NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989)).

[172] COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 113 (4th ed. 2012); *see*, *e.g.*, 18 U.S.C. § 1029(a) (prohibiting access-device fraud "if the offense affects interstate or foreign commerce"); 18 U.S.C. § 2510(12) (defining "electronic communication" to mean any "transfer of signs, signals, writing, images, sounds, data, or intelligence . . . that affects interstate or foreign commerce").

[173] COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 172, at 113–14; *see also* United States v. Sutcliffe, 505 F.3d 944, 952 (9th Cir. 2007) (noting, in context of prosecution under § 1028, that "it seems clear that use of the internet is intimately related to interstate commerce").

[174] *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 172, at 113; *see also* United States v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000); United States v. Cotton, 471 F.2d 744, 750 (9th Cir. 1973).

[175] Robert Kantner, *Protecting Trade Secrets Internationally Through a Comprehensive Trade Secret Policy: Trade Secret Is Increasing and the Need for a Protection Policy Is Unquestionable*, 59 PRAC. LAW. 17, 18 (2013).

[176] Lanham Act, 15 U.S.C. §§ 1051–141 (2012).

[177] Kantner, *supra* note 175, at 18.

[178] *Id.*

statute.[179] As international law scholar Georges Delaume explained more than a half-century ago: "[O]nce a statute is promulgated, it is irrelevant whether its scope is limited to the punishment of nationals or to that of foreigners . . . *provided there cannot be any doubt as to the legislative intent*."[180]

¶65 One enforcement path that unquestionably does apply to foreign defendants is to pursue a complaint of IP theft by filing a complaint with the ITC.[181] This is a standard route for companies seeking legal recourse for loss of trade secrets by foreign defendants,[182] particularly after the Federal Circuit's decision in *TianRui v. International Trade Commission and Amsted Industries*.[183] *TianRui* holds that under § 337 of the Tariff Act of 1930,[184] ITC relief is available to a domestic victim of trade secret theft even if the misconduct took place outside of the United States.[185]

¶66 In *TianRui*, a Chinese corporation stole trade secrets pertaining to the manufacture of cast-steel railway wheels.[186] TianRui attempted to negotiate with U.S.-based Amstead Industries to gain licensing rights to the method, but when negotiations failed, TianRui hired nine of Amsted's employees from its licensee, DACC, and using their knowledge of the product, produced wheels that were marketed and imported into the United States.[187] Amsted subsequently filed a complaint with the ITC.

¶67 TianRui sought to have the claim dismissed because the alleged trade secret misappropriation occurred in China,[188] arguing that Congress did not intend § 337 to apply extraterritorially.[189] However, the administrative law judge held the location of the misappropriation (China) was not the main issue in this case.[190] Using Illinois state law, the judge determined that TianRui unlawfully appropriated 128 trade secrets.[191]

¶68 On review, the court concluded that § 337 permits the ITC to apply state trade secret law to misconduct that took place in China. While there are some who believe that U.S. courts do not have the authority to address trade secret theft abroad,[192] *TianRui*

---

[179] Morrison v. Nat'l Austl. Bank, 130 S. Ct. 2869, 2873 (2010) (quoting EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)) ("It is a 'longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'"); *see* Columbia Broad. Sys. Inc. v. Scorpio Music Distribs., Inc., 569 F. Supp. 47, 49 (E.D. Pa. 1983), *aff'd mem*., 738 F.2d 424 (3d Cir. 1984) ("The protection afforded by the United States Code does not extend beyond the borders of this country unless the Code expressly states.").

[180] Blakesley, *supra* note 47, at 11 (emphasis added) (quoting Georges R. Delaume, *Jurisdiction over Crimes Committed Abroad: French and American Law*, 21 GEO. WASH. L. REV. 173, 181 (1952–53)).

[181] U.S. INT'L TRADE COMM'N, http://www.usitc.gov/ (last visited Sept. 6, 2014).

[182] *See* Viki Economides, Comment, TianRui Group Co. v. International Trade Commission*: The Dubious Status of Extraterritoriality and the Domestic Industry Requirement of Section 337*, 61 AM. U. L. REV. 1235 (2011) (discussing the limits of extraterritoriality under § 337).

[183] TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1325 (Fed. Cir. 2011).

[184] Tariff Act of 1930, Pub. L. No. 71-361, § 337, 46 Stat. 590 (codified as amended at 19 U.S.C. § 1337 (2006)).

[185] *TianRui Grp. Co.*, 661 F.3d at 1325; *see* Steven E. Feldman & Sherry L. Rollo, *Extraterritorial Protection of Trade Secret Rights in China: Do Section 337 Actions at the ITC Really Prevent Trade Secret Theft Abroad?*, 11 J. MARSHALL REV. INTELL. PROP. L. 523, 525 (2012).

[186] *TianRui Grp. Co.*, 661 F.3d at 1325.

[187] *Id.* at 1324.

[188] *Id.* at 1329.

[189] *Id.* at 1325; Feldman, *supra* note 185, at 530.

[190] *TianRui Grp. Co.*, 661 F.3d at 1325.

[191] *Id.*

[192] Economides, *supra* note 182, at 1243.

reflects the importance of finding viable domestic routes to protect IP and IT, particularly when such protection is difficult or impossible to find in foreign courts and agencies.

¶69 *TianRui* notwithstanding, the Supreme Court's policy regarding extraterritoriality is fairly clear: "When a statute gives no clear indication of extraterritorial application, it has none."[193] Even the requirement of establishing impact on a "domestic industry" component can be problematic. In *John Mezzalingua Associates, Inc. v. International Trade Commission*,[194] PPC, a coaxial-cable connectors manufacturer, filed a § 337 complaint with the ITC claiming the imported coaxial-cable connectors infringed on its patent design.[195] The ITC held that PPC had "failed to satisfy the 'domestic industry' requirement and PPC appealed."[196] Section 337 requires a "domestic industry," which in turn includes "(a) significant investment in plant and equipment; (b) significant employment or labor or capital; or (c) substantial investment in its exploitation, including engineering, research and development, or licensing."[197]

¶70 If careful to stay foreign, foreign companies that steal IP and IT benefit from the historic reluctance of American courts to reach beyond U.S. borders, notwithstanding the limited ITC process.[198]

C. Federal Initiatives

¶71 There are those who take the position that federal cases, certainly those mentioned above and brought pursuant to § 337 of the Tariff Act, "should be decided under a uniform federal standard, rather than by reference to a particular state's tort law."[199] This raises the question of whether federal law is a more viable option for pursuing foreign defendants than state law.

¶72 While the federal government has not given highest priority to the problem of IT and IP theft, there are indications of a renewed and meaningful commitment to addressing this problem, most notably the creation of the Office of the Intellectual Property Enforcement Coordinator and the Interagency Trade Enforcement Center.[200]

¶73 One federal agency, the Federal Trade Commission (FTC), has the authority to address unfair competition,[201] but despite a direct request from the National Association of Attorneys General urging the FTC to act, has failed to take significant enforcement

---

[193] *Id.* (citing Morrison v. Nat'l Austl. Bank, 130 S. Ct. 2869, 2878 (2010)).

[194] 660 F.3d 1322 (Fed. Cir. 2011).

[195] Gregory J. Spak et al., *A Review of Recent Decisions of the United States Court of Appeals for the Federal Circuit Area Summary: 2011 International Trade Law Decisions of the Federal Circuit*, 61 AM. U. L. REV. 1105, 1142 (2012) (citing *John Mezzalingua Assocs.*, 660 F.3d 1322).

[196] Spak et al., *supra* note 195, at 1143 (quoting *John Mezzalingua Assocs.*, 660 F.3d at 1324).

[197] *Id.* (citing 19 U.S.C. § 1137(a)(3) (2006)).

[198] *See*, *e.g.*, J. McIntyre Machinery, Ltd. v. Nicastro, 131 S. Ct. 2780 (2011); Goodyear Dunlop Tires Operations, S.A. v. Brown, 131 S. Ct. 2846, 2851 (2011); Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102, 113 (1987); Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 415–18 (1984); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 294 (1980); Hanson v. Denckla, 357 U.S. 235, 253 (1958); Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

[199] TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1327 (Fed. Cir. 2011).

[200] Ezell, *supra* note 17.

[201] 15 U.S.C. § 45(m)(1)(A) (2006) (allowing FTC to seek civil penalties from a company or person violating any such rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule").

action combatting the use of stolen IP and IT.[202] FTC jurisdiction includes actions committed abroad that have a "direct, substantial, and reasonably foreseeable effect" on domestic commerce at home.[203] Although the agency declined to act, Chairman Jon Leibowitz did issue a reply stating that the FTC is "deeply committed to exploring issues at the intersection of competition and intellectual property," and that the FTC is "always on the lookout for ways to use our broad . . . enforcement authority judiciously, yet effectively, to combat unfair methods of competition . . . within the scope of [its] jurisdiction . . . ."[204] It is hard to see how a pattern and practice of theft of IP and IT abroad causing billions of dollars in domestic losses and distorting the price of vast quantities of goods sold in the United States does not qualify as an unfair method of competition.

¶74 The Commission on the Theft of American Intellectual Property released a report in May 2013 proposing changes to U.S. policy to prevent China's appropriation of U.S. intellectual property.[205] The report recommended the FTC "obtain meaningful sanctions against foreign companies using stolen IP."[206] It remains to be seen whether this recommendation will prompt the FTC to take action.

¶75 Beyond the FTC, Stephen Ezell, an IT commentator with the Information Technology and Innovation Foundation, suggests that the United States needs to make apparent that systematic theft of U.S. IP will have consequences.[207] "[T]he Secretary of the Treasury should be empowered to deny the use of the American Banking system to foreign companies that repeatedly use or benefit from the theft of American IP, even if Wall Street objects."[208] He also suggests more of a focus on major offenders, including China, and amendments to the Economic Espionage Act to create "a federal right of action for trade-secret theft."[209] Ezell also urges granting customs officials greater authority to impound at the border exports they suspect have benefitted from IP theft.[210]

¶76 Part of the federal interest in this field lies in the direct linkage between IP and IT theft and national security. Section 833 of the 2013 National Defense Authorization Act (NDAA)[211] addresses IP and IT counterfeiting with the goal of keeping pirated products out of the supply chain for goods available or sold in the United States. Counterfeiting,

---

[202] Letter from the Nat'l Ass'n of Att'ys Gen. to the FTC (Nov. 4, 2011), *available at* http://www.naag.org/assets/files/pdf/signons/FTCA percent20Enforcement percent20Final.PDF.

[203] 15 U.S.C. § 45(a)(3)(A)(i)(ii) (2006) ("This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless—(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect . . . ."); *see* Michael A. Rabkin, *When Consumer Fraud Crosses the International Line: The Basis for Extraterritorial Jurisdiction Under the FTC Act*, 101 NW. U. L. REV. 294, 296 (2007); *see also* Richard W. Beckler & Matthew H. Kirtland, *Extraterritorial Application of US Antitrust Law: What Is a "Direct, Substantial, and Reasonably Foreseeable Effect" Under the Foreign Trade Antitrust Improvements Act?*, 38 TEX. INT'L L.J. 11 (2003) (reviewing the "effects" test as it applies, *inter alia*, to the FTC).

[204] Grant Gross, *Update: Senators Press FTC to Begin Investigating Software Piracy*, CFO WORLD (Apr. 3, 2012), http://www.cfoworld.com/technology/35677/update-senators-press-ftc-begin-investigating-software-piracy.

[205] IP COMMISSION REPORT, *supra* note 5, at 14.

[206] *Id*. at 6.

[207] Ezell, *supra* note 17.

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] H.R. 4310, 112th Cong. (2d Sess. 2013).

like all forms of IP and IT theft, undermines critical forces in the U.S. economy, lessens incentives for product and service improvement, decreases interest in investment in U.S. initiative and innovation, and can compromise national security.[212] The Department of Defense has recognized that pirated or reverse-engineered copies function less reliably and can be "programmed with hidden spyware or backdoors for espionage."[213] These concerns are also evident "in-house," as noted in the IP Commission Report mentioned earlier,[214] which discussed the discovery of 1,800 counterfeit electronic components within the supply chain of the U.S. Department of Defense.[215]

¶77 Beyond the NDAA, the Economic Espionage Act (EEA)[216] criminalizes certain trade secret theft[217] and allows the "U.S. Attorney General to initiate civil public enforcement proceedings."[218] The EEA applies only to a "U.S. citizen or permanent resident alien or an organization organized under U.S. law, or if an act in furtherance of the offense was committed in the United States."[219] This limits EEA enforcement and can preclude its use for many types of IT and IP theft in global supply chains that harm U.S. interests but take place beyond the border.[220] However, there is a general argument that foreign defendants engaged in a conspiracy with domestic co-conspirators located in the United States are within the jurisdictional reach of the courts,[221] limiting enforcement to those instances where (a) the restrictive requirements of the Act are met and (b) a federal agency exercises its discretion to initiate an enforcement action.

¶78 Naturally, the overall picture of federal interests requires consideration of U.S. Immigration and Customs Enforcement (ICE).[222] ICE leads the National Intellectual Property Rights Coordination Center (IPR Center),[223] and "stands at the forefront of the U.S. Government's response to global intellectual property theft."[224] Although ICE, the Department of Justice, and the FBI have considerable authority under the EEA to deal with IP and IT theft, *United States v. Aleynikov*, mentioned earlier,[225] illustrates important limitations on federal prosecution.[226] Aleynikov, a former employee of Goldman Sachs &

---

[212] *See* Ezell, *supra* note 17; *see also* Barnett, *supra* note 10, at 856–7 (finding that if reverse engineering were held as a constant for preventing counterfeiting, patents would enable innovation).

[213] Steve Charles, *DOD Gets Serious About Supply Chain Security*, WASH. TECH. (Feb. 27, 2013), http://washingtontechnology.com/articles/2013/02/27/insights-charles-supply-chain-security.aspx.

[214] Ezell, *supra* note 17.

[215] IP COMMISSION REPORT, *supra* note 5, at 12.

[216] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39.

[217] ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, *supra* note 9, at 1, 19.

[218] *Id*.

[219] *Id*. at 20.

[220] Add to this the fact that U.S. copyright law typically does not have extraterritorial jurisdiction. *See*, *e.g*., Quality King Distrib., Inc. v. L'Anza Research Int'l, 523 U.S. 135, 154 (1998) (Ginsburg, J., concurring).

[221] *See generally* ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, *supra* note 9.

[222] *See* IMMIGRATION & CUSTOMS ENFORCEMENT, http://www.ice.gov (last visited Apr. 18, 2014).

[223] NAT'L INTELLECTUAL PROP. RIGHTS COORDINATION CTR., http://www.iprcenter.gov (last visited Apr. 18, 2014).

[224] Council for Trade-Related Aspects of Intellectual Property Rights, *Securing Supply Chains Against Counterfeit Goods*, IP/C/W/570 (May 31, 2012).

[225] *See supra* note 135 and accompanying text.

[226] United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012); *see* Kenneth W. Taber & Ranah L. Esmaili, *Congress Raises the Stakes for Theft of Trade Secrets with Passage of Two New Laws*, PILLSBURY LAW

Co., was convicted of "stealing and transferring some of the proprietary computer source code used in his employer's high frequency trading system, in violation of the National Stolen Property Act[227] . . . and the Economic Espionage Act."[228] Aleynikov appealed, claiming the product was not "produced for or placed in interstate or foreign commerce."[229] The court agreed and reversed the lower court's decision.[230]

¶79 Reacting to this decision, Congress passed the Theft of Trade Secrets Clarification Act of 2012, replacing "a product that is produced for or placed in interstate or foreign commerce," with "a product or service *used in* or intended for use in interstate or foreign commerce."[231] Congress followed with the Foreign and Economic Penalty Enhancement Act of 2012,[232] increasing the penalties in trade secret cases for those who "knowingly commit economic espionage to benefit a non-U.S. government, agency or instrumentality."[233] The fine was increased from $500,000 to $5,000,000[234] for individuals, and from $10,000,000 to "the greater of $10,000,000 or 3 times the value of the stolen trade secret"[235] for organizations. The Act also charges the United States Sentencing Commission to evaluate, when appropriate, "amending the federal sentencing guidelines for foreign trade secret theft convictions."[236]

¶80 Thus far, the new language in the EEA has led to a few prosecutions, though the number and nature of the cases are unlikely to change the IP- and IT-theft landscape.[237] The small number and infrequency of these cases is a testament to their cost,[238] complexity, and limited range. That is not to diminish their importance, but rather, to observe that federal or state efforts alone will not achieve the desired result of cutting or eliminating IP and IT theft.

(Feb. 11, 2013), http://www.pillsburylaw.com/publications/congress-raises-the-stakes-for-theft-of-trade-secrets-with-passage-of-two-new-laws.

[227] 676 F.3d 71, 73; 18 U.S.C. § 2314.

[228] 676 F.3d 71, 73; 18 U.S.C. § 1832.

[229] 676 F.3d 71, 73; 18 U.S.C. §§ 1831–39.

[230] 676 F.3d 71, 82.

[231] Taber, *supra* note 226 (citing Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627).

[232] *Id*. (citing Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442).

[233] *Id.*

[234] *Id*.

[235] *Id.*

[236] *Id*.

[237] *See*, *e.g*., United States v. Hanjuan Jin, 733 F.3d 718, 722 (7th Cir. 2013) (holding IP-theft case results in a five-year prison sentence); United States v. Nosal, 2013 WL 4504652, at *26 (N.D. Cal. Aug. 15, 2013) (denying a motion to acquit after a conviction in IP-theft case). *See generally* United States v. Liew, 2013 WL 2605126 (N.D. Cal. June 11, 2013) (pending IP-theft case).

[238] *See* Yu, *supra* note 23, at 242; Letter from William G. Barber, President, Am. Intellectual Prop. Law Assoc., to Hon. Victoria A. Espinel, U.S. Intellectual Prop. Enforcement Coordinator 2–3 (Aug. 10, 2012), *available at* http://www.aipla.org/advocacy/executive/Documents/AIPLA%20Comments%20to%20IPEC%20on%20Joint%20Strategic%20Plan%20on%20IP%20Enforcement%20-%208.10.12.pdf (responding to OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB-2012-0004-0002, REQUEST FOR PUBLIC COMMENTS: DEVELOPMENT OF THE JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT (2012)).

D. International Efforts

¶81 An Intellectual Property Commission Report released in May 2013 began with a general discussion of the continuing problem of IP and IT theft globally, raising the challenge of federal short-term measures and the possibility of legal reforms.[239] In some of the countries where threats to IP and IT are greatest, there is little evidence of a culture of compliance.[240] In those countries, "[j]udicial resources are either not utilized or lack the capacity or experience to hear cases."[241] Likewise, there are few criminal sanctions for IP and IT pirates in several countries where the violations are rife.[242]

¶82 The two most populous nations in the world, India and China, appear to have inefficient judicial institutions and seldom impose sufficient criminal sentences to deter IP theft.[243] In China, the courts are overwhelmed with cases, and judges with jurisdiction over IP cases are spread thin.[244] Barriers to service of process, discovery, and meaningful remedies in both countries remain a vexing problem for U.S. parties seeking redress, both there and in U.S. courts.[245] Despite improvements in some sectors following China's 2010 Special IPR Enforcement Campaign,[246] China remained on the "priority watch list" published by the United States Trade Representative (USTR)[247] in 2012 and 2013.[248]

¶83 A Business Software Alliance (BSA) study denotes software piracy as a vast and dangerous international problem,[249] which is likely to continue to grow because "emerging economies, which in recent years have been the driving force behind PC software piracy, are now decisively outpacing mature markets in their growth rate."[250] In 2011, emerging economies "account[ed] for more than half of all PCs in use."[251]

¶84 Given the nature of the problem, it is worth asking whether the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS),[252] the primary multilateral agreement in the field, provides reliable resolution of trans-boundary IP and IT theft. All World Trade Organization (WTO) members are party to TRIPS, which sets out rules for copyrighted materials, trademarks, geographic indications (e.g., for region-specific wine or cheese), industrial design, patents, and other IP and IT interests.[253]

---

[239] *See* IP COMMISSION REPORT, *supra* note 5, at 14.
[240] *See id.*
[241] *Id.*
[242] *See id.*
[243] *See id.*
[244] *See id.*
[245] *See id.* (citing Allison Walton & Dean Gonsowski, *Like the Great Wall: E-discovery Barriers Still Exist Between the U.S. and China*, INSIDE COUNSEL (Dec. 3, 2012), http://www.insidecounsel.com/2012/12/03/like-the-great-wall-e-discovery-barriers-still-exi.
[246] China announced a six month campaign to reduce IP theft and recently agreed to make this effort permanent. Press Release, U.S. Dep't of Commerce, U.S. and China Conclude 22nd Session of the Joint Commission on Commerce and Trade (Nov. 21, 2011).
[247] IP COMMISSION REPORT, *supra* note 5, at 14 (citing OFFICE OF THE U. S. TRADE REPRESENTATIVE, 2012 SPECIAL 301 REPORT (2012), and OFFICE OF THE U. S. TRADE REPRESENTATIVE., 2013 SPECIAL 301 REPORT (2013)).
[248] *Id.*
[249] BUS. SOFTWARE ALLIANCE, *supra* note 20, at 1.
[250] *Id.*
[251] *Id.*
[252] TRIPS, *supra* note 61.
[253] *See Overview: The TRIPS Agreement*, WORLD TRADE ORG., http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (last visited Oct. 5, 2014).

¶85 TRIPS requires state parties to develop enforcement procedures with meaningful remedies, including injunctions and other measures, to sanction violators and deter further infringement.[254] The agreement allows only for those damages necessary to compensate the injury caused by the infringement plus the possibility of legal costs.[255] It also requires state parties to "provide for criminal procedures and penalties to be applied at least in cases of willful trademark counterfeiting or copyright piracy on a commercial scale."[256]

¶86 TRIPS is written to accommodate new signatories, and delays the start of state obligations for one year after entry into the WTO.[257] It gives developing countries or countries transitioning from a centrally planned economy into a free-enterprise economy a compliance delay of four years after securing WTO membership.[258] The compliance delay extends to five years if there is a need to develop and implement protections for patentable goods, assuming such provisions were not in place prior to entering the WTO.[259] The delay extends to ten years for members that qualify as least-developed countries.[260] TRIPS requires developed countries to provide incentives to new developing-country members to facilitate both IP protection and technology transfer.[261] These delayed enforcement provisions raise legitimate questions about the resolve reflected in TRIPS and the value or merit of WTO sanctions.[262]

¶87 The 2011 Anti-Counterfeiting Trade Agreement (ACTA)[263] has a more declarative text but, as critics have pointed out, the negotiation process underlying its use and implementation lacks transparency.[264] Add to this the general lack of trade secrets protection in many countries where trade secrets "are either not at all, or are inadequately, protected,"[265] and one gets a sense of the incomplete nature of both ACTA and TRIPS. Accordingly, "Once a trade secret is made public, it enters the public domain. Invariably it will be lost permanently and, in most instances, so will the competitive advantage linked to it."[266] Based on recent surveys, this hazard is particularly pronounced in China, Pakistan, Russia, and India.[267]

¶88 China, a signatory to a number of the aforementioned agreements, accounts "for 50 to 80 percent globally" of IT and IP theft.[268] IP protection in India has also raised

---

[254] *See id.*

[255] Parties must also show that infringer did so knowingly, or in the alternative, that the perpetrator was reasonably likely to know that he was infringing upon such rights. TRIPS, *supra* note 61, art. 45. Article 45 of TRIPS addresses damages and is narrower than the 2011 Anti-Counterfeiting Trade Agreement (ACTA). *See* Anti-Counterfeiting Trade Agreement, Oct. 1, 2011 [hereinafter ACTA], *available at* http://www.ustr.gov/acta (summarizing ACTA).

[256] TRIPS, *supra* note 61, art. 61.

[257] Articles 65 and 66 of TRIPS extend the time frame for compliance for as long as ten years for developing countries. *See* TRIPS, *supra* note 61, art. 65, 66.

[258] TRIPS, *supra* note 61, art. 65, ¶ 2.

[259] *Id*. ¶ 4.

[260] *Id.* art. 66.

[261] *Id*.

[262] Yu, *supra* note 23, at 243.

[263] ACTA, *supra* note 255.

[264] Rens, *supra* note 19, at 784–85.

[265] GHELFI, *supra* note 46, at 8.

[266] *Id.*

[267] *See* Almeling, *supra* note 45, at 1111.

[268] Ezell, *supra* note 17.

questions about the value and success of multilateral agreements.[269] Among other things, India's Ministry of Commerce's Technology Import and Export Regulations appear to vest something resembling IP ownership in an employee who plays a central role in its development.[270] Under this interpretation, improvements to technology downstream the supply chain are difficult to protect and the overall IP-rights formulation becomes murky at best.

¶89 In the European Union (EU), IP infringement can be pursued through Article 7(1)(b) of Directive 2009/24/EC on the legal protection of computer programs.[271] The Directive obligates member states to "provide . . . appropriate remedies against a person committing [an] act of . . . the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy."[272] The EU recognizes the importance of IP theft, and the Council Resolution on the EU Customs Action Plan sets out a plan to dedicate 2013–2017 to tackling IP infringement.[273]

¶90 In sum, the EU commonly adopts multinational approaches to combat trade-related issues. Further, a number of countries, including the United States,[274] have enacted or are in the process of implementing similar measures specifying that government ministries may only use legitimate software.[275]

E. Private Efforts

¶91 Beyond state, federal, and international regimes to protect IP and IT, there are various private entities playing a role in this fight. Each of these companies or services described below, like all of the state, federal, and multinational legal enforcement mechanisms discussed earlier, address the reality of 21st century business: success in

---

[269] *See* Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?,* 21 TEMP. INT'L & COMP. L.J. 103, 127–28 (2007).

[270] CTR. FOR RESPONSIBLE ENTER. & TRADE, TRADE SECRET THEFT: MANAGING THE GROWING THREAT IN SUPPLY CHAINS 11–12 (2012), *available at* http://create.org/resource/trade-secret-theft-managing-the-growing-threat-in-supply-chains/.

[271] *See id*.

[272] MITCHELL III ET AL., *supra* note 73, at 13 (citing Council Directive 2009/24, 2009 O.J. (L 111) 16 (EC)). This directive does not address whether only the person directly using the software can be held accountable or if there is any downstream liability. *See id.* "In two recent cases decided related to online services, the Court held that a reference system provider and an operator of an online marketplace cannot escape liability where they knew of the infringement and did not act." *Id.* at 14 (citing as an example, Case C-324/09, L'Oréal SA v. eBay I, Celex No. 609CC0324 (Dec. 9, 2010)).

[273] *Id.* at 14 (citing Council Resolution on the EU Customs Action Plan to Combat IP Infringement for the Years 2013 to 2017, 2013 O.J. (C 80) 1).

[274] *See* Ezell, *supra* note 17. "Procurement of genuine software has also been a focus for policymakers: Executive Order 13103 of September 30, 1998 requires U.S. government agencies to maintain procedures to ensure that they use only authorized business software." Exec. Order No. 13,103, 63 Fed. Reg. 53, 273 (Oct. 5, 1998), *available at* http://www.gpo.gov/fdsys/pkg/FR-1998-10-05/pdf/98-26799.pdf. See also, for example, Council Regulation 1907/2006, 2006 O.J. (L 396) 1 (EC), which provides an outline of the EU's multinational REACH regulation on chemicals that requires most manufacturers and importers of products, including electronic components, to provide appropriate safety information about hazardous substances in their products.

[275] These countries include Bolivia, Chile, China, Colombia, Costa Rica, the Czech Republic, France, Greece, Hong Kong, Hungary, Ireland, Israel, Jordan, South Korea, Lebanon, Macau, Paraguay, Peru, the Philippines, Spain, Taiwan, Thailand, Turkey, and Vietnam. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2008 SPECIAL 301 REPORT 12 (2008).

almost any field requires disclosure of valuable IP and IT. For knowledge-based outsourcing involving specialized domain expertise, the company is invariably required "to disclose and share knowledge-intensive processes with the offshore provider, which knowledge may be in the form of proprietary technology, software, chemical entities, specifications, product designs, business processes, methodologies, drug formulations or other sensitive data."[276] In light of this, companies should make efforts to retain control over daily operations within the supply chain and protect intellectual property, though, significant risks will inevitably remain.[277]

¶92 Most supply chains rely on third-party sourcing, and that often means relinquishing control, thus exposing proprietary IP and IT. In one case, a Chinese electronics manufacturer paid an employee of Apple-supplier Foxconn approximately $3,000 for information and images of the iPad 2, so that it could make protective cases for the iPad 2 several months before the product's release.[278] The value of the R&D connected with the stolen trade secret is estimated to be worth 100 times more than the money the employee received.[279] In this instance, the employee was caught, tried, and incarcerated in China.[280]

¶93 Private employers not only must implement internal policies to prevent IP theft, but can also pursue a private cause of action under the Computer Fraud and Abuse Act (CFAA)[281] against former employees who have stolen trade secrets from company computers.[282] This remedy is somewhat limited, particularly after the Ninth Circuit's decision in *United States v. Nosal*.[283] The court in *Nosal* held that "an employee could not be liable under the CFAA for 'exceeding authorized access' to an employer's computer by accessing proprietary information in violation of the employer's written computer use policies."[284] In *Nosal*, a former employee "allegedly convinced several former colleagues to download and transmit lists of executives so that he could compete with this former employer."[285] The court found, "[The CFAA] prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."[286] In addition, the Fourth

---

[276] SONIA BALDIA, MAYER, BROWN, ROWE, & MAW, THINKING OUTSIDE THE BPO: KNOWLEDGE PROCESS OUTSOURCING TO INDIA 4 (2007–8), *available at* http://www.offshoringtransparency.org/resources/ThinkingOutsidetheBPO.pdf.

[277] *See* MITCHELL III ET AL., *supra* note 73, at 15.

[278] Michael Kan, *Chinese Court Sentences Three to Prison for IPad Design Leak*, PC WORLD (June 15, 2011), http://www.pcworld.com/article/230406/article.html.

[279] *See id.*

[280] *See id.*

[281] 18 U.S.C. § 1030 (2008) ("[Applies to those who] knowingly accessed a computer without authorization or exceed[ed] authorized access . . . ."); *see also* § 1030(g) (providing a private cause of action).

[282] *See* Illana S. Rubel & Sebastian E. Kaplan, *CFAA Is Losing Ground as a Tool to Fight Trade Secret Misappropriation*, LEXOLOGY (Aug. 27, 2012), http://www.lexology.com/library/detail.aspx?g=1db80ea9-df54-420f-9e81-881aafcacd6e.

[283] 676 F.3d 854 (9th Cir. 2012).

[284] Rubel, *supra* note 282; *see Nosal*, 676 F.3d at 857 ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.").

[285] Rubel, *supra* note 282; *see Nosal*, 676 F.3d at 856.

[286] *Nosal*, 676 F.3d at 863 (quoting Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010)).

Circuit adopted a similar stance in *WEC Carolina Energy Solutions LLC v. Miller*, which mirrors the court's reasoning in *Nosal*.[287]

¶94 Rather than providing a needed remedy for IP-theft victims, *Nosal* expresses concern about criminalizing innocuous activity.[288] This case is troubling for those attempting to address theft of trade secrets since the court found the CFAA to be almost solely an anti-hacking statute, not one designed to address misappropriation of trade secrets or other forms of IP and IT theft. The statute's general purpose, the court noted, is "to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets."[289] This perverse interpretation of the CFAA, coupled with jurisdictional limitations and weak enforcement regimes, underscores the importance of alternative or nongovernmental measures to protect IP and IT.

¶95 Given the scattered and unreliable remedial potential of Article III Courts, private organizations have emerged to help IP owners protect their property. FACT, a private company based in Great Britain, is set up exclusively to combat piracy of intellectual property.[290] Under the FACT Certification Scheme, which currently covers over 110 companies, businesses "must satisfy members they have sufficiently high levels of security in order to safeguard the intellectual property rights of FACT members."[291] FACT represents entities in the "film, television, technology and sports rights industries."[292]

¶96 In the United States, Verafirm provides a certification system designed to communicate that an IP user is legal, licensed, and not engaging in IP theft. Verafirm certification is a "first step in demonstrating that your company is transparent, well-run, and respects intellectual property."[293] Verafirm's system has varying levels of certification, each designed to indicate increasing levels of scrutiny and protection of IP and IT.[294]

¶97 The Global Intellectual Property Center has developed a manual to assist businesses in protecting their intellectual property from misappropriation.[295] The Center warns: "Counterfeiters prey on companies with lax security measures and porous supply chains . . . counterfeiters have an uncanny ability to detect weaknesses in a brand owner's supply chain and frequently point to those weaknesses when accused of counterfeiting."[296] The Center functions as an advocacy body within the Chamber of Commerce and does not have enforcement power.[297]

---

[287] *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206–07 (4th Cir. 2012).
[288] *Nosal*, 676 F.3d at 859.
[289] *Id.* at 863.
[290] *FACT Certification*, FACT, http://factcertification.com (last visited Aug. 15, 2013).
[291] *Id.*
[292] *Id*.
[293] *About Verafirm*, VERFIRM, https://www.verafirm.org/Pages/General/About.aspx (last visited Sept. 5, 2014).
[294] *Id.* (outlining different levels of certification as Verafirm-Registered, Verafirm-Verified, and Verafirm-Certified).
[295] *See* GLOBAL INTELLECTUAL PROP. CTR., INTELLECTUAL PROPERTY PROTECTION AND ENFORCEMENT MANUAL: A PRACTICAL AND LEGAL GUIDE FOR PROTECTING YOUR INTELLECTUAL PROPERTY RIGHTS (2009).
[296] *Id.* at 11.
[297] *See id*. at 52.

¶98 The Center for Responsible Enterprise and Trade (CREATE.org)[298] works with multinational corporations to improve business practices in global supply chains while protecting intellectual property rights.[299] CREATE.org offers "best practices"[300] for the industry and government procurement officials to help detect counterfeiting and ensure product safety.[301]

¶99 The Internet Crime Complaint Center (IC3) is a partnership between the U.S. Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).[302] NW3C provides nationwide support systems for law enforcement and regulatory agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime.[303] The IC3 was renamed in October 2003 to reflect both its reach into Internet abuse and cybercrime, and its mission to receive, develop, and refer criminal cybercrime complaints. After ten years, although there have been some victories, IC3 has not made a meaningful dent in the range and frequency of IT and IP theft.

¶100 The massive impact of IP and IT theft described at the outset of this Article stands as a testament to the insufficiency of existing measures. It is not that any one of the above entities or the legal remedies discussed earlier is without merit; it is that each entity acts in isolation.[304] Further, it is next to impossible to stop IT and IP theft in a world where huge segments of the population do not view unauthorized file-sharing, downloading critical information to a thumb drive, or other nearly invisible acts of piracy as criminal or even wrongful.

¶101 Successful case-by-case enforcement deterring large numbers of people from piracy is impossible in a world that has not fully bought into the simple, underlying premise that stealing IP and IT in any form is wrong. When Chinese and U.S. college students, along with technology workers in India and Indiana, simply do not accept that IT and IP theft is wrong, and believe it is, at worst, a victimless crime, the probability of a substantial reduction in theft brought on by fear of enforcement is very low.[305]

¶102 It may be, in the end, that this set of problems will only abate when public attitudes about IP and IT theft begin to shift. There are some signs that as a matter of personal

---

[298] CTR. FOR RESPONSIBLE ENTER. & TRADE, http://www.create.org/ (last visited Sept. 5, 2014).

[299] *See* DARREL M. WEST, TWELVE WAYS TO BUILD TRUST IN THE ICT GLOBAL SUPPLY CHAIN 10 (2013).

[300] CTR. FOR RESPONSIBLE ENTER. & TRADE, HEALTH AND SAFETY RISKS, *supra* note 55, at 18–19.

[301] The Center for Responsible Enterprise & Trade's goals are to 1) insure greater traceability in the supply chain, 2) foster greater cooperation, coordination, and accountability among all participants, 3) increase information sharing to strengthen supply-chain integrity, 4) include provisions in supplier contracts that facilitate and improve oversight, 5) calibrate supplier assessments according to risk level, 6) engage proactively with suppliers on an ongoing basis, 7) ensure that supplier requirements flow down to subcontractors, 8) develop procedures for reporting on and ensuring destruction of counterfeit parts, 9) work collaboratively with government authorities to support product safety and quality, and 10) increase awareness among consumers and end users about the hazards of counterfeits. *Id.* at 18–19.

[302] *See* INTERNET CRIME COMPLAINT CTR., http://www.ic3.gov/default.aspx (last visited Sept. 5, 2014).

[303] *See id*.

[304] Trevor T. Moores, *An Analysis of the Impact of Economic Wealth and National Culture on the Rise and Fall of Software Piracy Rates*, 81 J. OF BUS. ETHICS 39, 47 (2008) (discussing how the certainty of punishment reduces the probability of piracy).

[305] *See* George E. Higgins, Abby L. Wilson, & Brian D. Fell, *An Application of Deterrence Theory to Software Piracy*, 12(3) J. CRIM. JUSTICE & POPULAR CULTURE 166, 178–79 (2005) ("[W]e believe there is a culture that thinks software piracy is proper behavior, but if educational institutions can change this climate to emphasize the criminogenic issues surrounding software piracy, then the behavior may be reduced.").

ethics, consumers value the IP and IT integrity of the companies and entities with whom they deal.[306] That belief structure is obviously not adopted as a universal and fundamental value. Without that shared understanding, vulnerabilities not only continue—they increase.

¶103 Taken together, the mechanisms discussed thus far can go a long way in protecting IP and IT. Governments and private actors are and should be increasingly focused on preventing trade secret theft through industrial and economic espionage, as well as cyber espionage.[307] Companies need effective compliance programs to manage IP risks. Yet notwithstanding these well-known financial repercussions, businesses often neglect to properly allocate adequate resources to such programs. For instance, in many companies, compliance programs for anticorruption are more developed than those for IP protection.[308]

IV. THE ESSENTIAL NATURE OF A PUBLIC AND PRIVATE-SECTOR PARTNERSHIP

¶104 Given the magnitude of the problem in the United States, one would think that all branches of government and all businesses with IP exposure would be engaged, strategizing on ways to combat the IP and IT theft that drains hundreds of billions in value, however calculated, every year. That assumption, however, is not entirely correct. Many governmental entities, such as the FTC, have not entered the fray.

¶105 As to private-sector actors, a recent study by Setec, Inc., an independent provider of vendor-neutral information-security solutions, noted:

> With 70 percent of the world's intellectual property within the United States, US-based companies continue to dedicate extensive resources to research and development . . . . [But recent studies] demonstrate that over one-third of surveyed Fortune 2000 and middle-market companies have no

---

[306] *See Why Are Americans Afraid of China?*, NAT'L PUB. RADIO (June 5, 2013), http://www.npr.org/templates/story/story.php?storyId=188919258. Bruce Pickering of the Asia Society stated:

> [T]here are sometimes competing priorities because the American consumer, on the one hand, wants inexpensive products. That's why the Chinese have, you know, so much of our trading has been with China is that they've been able to produce so many products Americans want comparatively inexpensively. And there is a concern, I think, on the part of companies that also, though, the American consumer doesn't just simply want products without any kind of ethical, you know, handling. And the more they know, of course, the more likely people are to make educated choices. So I think, when operating in Asia, given a choice, Americans would like to get low-cost products with ethical, you know, kind of ethical sourcing. And when information comes out, they tend to make decisions, I think, that move away from, you know, kind of workplace conditions that are inhuman or at least not very nice.

Id.

[307] IP COMMISSION REPORT, *supra* note 5, at 39.

[308] *See* BAYER, *supra* note 16, at 30–36.

> formal program for safeguarding intellectual property and spend less than 5% of their budgets on security.[309]

¶106 The absence of thorough public or governmental protection and limits on private action produce a vacuum in which IP and IT theft thrives. A collaborative public/private partnership with comprehensive industry participation can harness the resources of many actors and entities. At the domestic level, organizations like the National Alliance for Jobs and Innovation (NAJI)[310] hold great promise for a global solution. It is time for a multinational approach with unified goals.

¶107 In February 2013, the Executive Office of the President released the "Administration Strategy of Mitigating the Theft of U.S. Trade Secrets," which urges increasing diplomatic efforts, promoting best practices within private industries, enhancing domestic law enforcement, pursuing legislative initiatives, and increasing public awareness.[311] Additionally, multiple guidelines focus on protecting trade secrets from misappropriation rather than addressing opportunities for recourse following the theft of IP. The report highlights the importance of "logistical controls" and "[s]ecurity, especially in the electronic environment."[312]

¶108 The 2013 IP Commission Report provides a comprehensive source of specific recommendations for legislative and legal reform.[313] Entities in the private sector have

---

[309] *Investigating Intellectual Property Theft*, SETEC INVESTIGATIONS, http://www.setecinvestigations.com/resources/whitepapers/whitepaper5.php (last visited Sept. 5, 2014).

[310] NAT'L ALLIANCE FOR JOBS & INNOVATION, http://naji.org/ (last visited Sept. 5, 2014). Disclosure note: author currently sits on the board of the National Alliance for Jobs and Innovation.

[311] *See* ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, *supra* note 9.

[312] *Id.* at 9.

[313] IP COMMISSION REPORT, *supra* note 5. The Report further recommends that private entities:

> Designate the national security advisor as the principal policy coordinator for . . . the protection of American IP . . . .
>
> Provide statutory responsibility . . . to the Secretary of Commerce to serve as the principal official to manage all aspects of IP protection . . . .
>
> Strengthen the International Trade Commission's 337 process to sequester goods containing stolen IP . . . .
>
> Empower the Secretary of the Treasury . . . to deny the use of the American banking system to foreign companies that repeatedly use or benefit from the theft of American IP . . . .
>
> Increase Department of Justice and Federal Bureau of Investigation resources to investigate and prosecute cases of trade-secret theft, especially those enabled by cyber means . . . .
>
> . . . .
>
> Enforce strict supply-chain accountability for the U.S. government . . . .
>
> Require the Securities and Exchange Commission to judge whether companies' use of stolen IP is a material condition that ought to be publicly reported . . . .
>
> . . . .
>
> Amend the Economic Espionage Act (EEA) to provide a federal private right of action for trade secret . . . .
>
> Make the Court of Appeals for the Federal Circuit (CAFC) the appellate court for all actions under the EEA . . . .
>
> Instruct the Federal Trade Commission (FTC) to obtain meaningful sanctions against foreign companies using stolen IP . . . .
>
> . . . .
>
> Build institutions in priority countries that contribute toward a "rule of law"

their own cut on the best approach. CREATE.org, mentioned earlier, offers similar proactive measures to reduce the risk of, *inter alia*, trade secret theft.[314]

¶109 Assuming some or many of these measures will be implemented, the fact remains that the problem of IP and IT theft exists at every level of the social and economic order. Ultimately, there are ethical considerations that underlie every purchase choice raising these questions:

(1) In some settings within and outside the United States, in countries where the financial, personal, and marketplace gains of stealing IP and IT greatly outweigh the risk of detection and sanction, will sporadic enforcement in the United States or local courts make a meaningful difference in rates of IT and IP theft?

(2) Both in the United States and abroad, is the integrity of IP and IT a meaningful factor in deciding on the choice of goods and services or does the lower cost of a pirated product outweigh the importance of compliance with the rule of law?[315]

(3) In those countries where there is little or no protection for trade secrets or confidential proprietary commercial information, is it realistic to expect that consumers will use IP integrity as a central variable in buying choices?[316]

(4) In countries where the government condones or participates in trade secret theft, will consumers, *sua sponte*, view IP integrity as important?[317]

> environment in ways that protect IP . . . .
>
> Develop a program that encourages technological innovation to improve the ability to detect counterfeit goods. Prize competitions have proved to be both meaningful and cost-effective ways to rapidly develop and assess new technologies . . . .
>
> Establish in the private, nonprofit sector an assessment or rating system of levels of IP legal protection, beginning in China but extending to other countries as well . . . .
>
> . . . .
>
> Support American companies [to] identify and recover IP stolen through cyber means.

Id. at 4–6.

[314] CTR. FOR RESPONSIBLE ENTER. & TRADE, TRADE SECRET THEFT, *supra* note 270, at 21. "[C]ompanies should: (1) conduct a strategic assessment of the company's trade secrets, (2) undertake appropriate pre-contractual due diligence, (3) employ strong contractual protections, backed by enforceable audit rights and penalties, (4) utilize appropriate operational and security measures, and (5) take appropriate action after the business relationship has ended." *Id*. The first measure suggests that a company "[e]stablish an internal trade secrets policy," "[i]ntegrate into the company's supplier code of conduct," and "[c]onsider which trade secrets should be transferred to suppliers." *Id.* at 22. The second measure suggests that a company "[c]onduct an assessment to ensure that potential suppliers are able to protect the company's secrets" and "[e]valuate other IP-related issues." *Id.* at 23. The fourth measure suggests that a company "[b]uild a culture of compliance" and use "[t]echnological safeguards." *Id.* at 24. For example, technological safeguards such as special codes, encryptions, etc., would fulfill the fourth measure's protective goal. *Id.* The fifth measure suggests that a company "[r]emind departing employees of their continuing obligation not to disclose trade secrets" and "[e]nsure that former business partners do not leak trade secrets." *Id.* at 25.

[315] *See* Thorin Klosowski, *Why I Stopped Pirating and Started Paying for Media*, LIFEHACKER (Mar. 14, 2013, 8:00 AM), http://lifehacker.com/5990525/why-i-stopped-pirating-and-started-paying-for-media. Sometimes, consumer choice is affected by a quality differential. For example, certain types of cloud software offer digital downloads across multiple devices, while pirated versions do not, making them less appealing to consumers. *See id.*

[316] *See* Sonia Baldia, *Intellectual Property in Global Sourcing: The Art of the Transfer,* 38 Geo. J. Int'l L. 499, 506, 510–11 (2007).

[317] *See* CTR. FOR RESPONSIBLE ENTER. & TRADE, TRADE SECRET THEFT, *supra* note 270, at 19.

(5) If IP owners have few options beyond public shaming[318] or boycotting companies that take advantage of unauthorized IP, does it seem likely that a regime of IP protection will spring into existence?[319]

¶110 Since the answer to these admittedly slanted questions is no, the need for self-help (an inexact methodology at best) has prompted private-sector law firms to craft advice and warning lists for their clients who have global IP and IT exposure.[320] Where they can afford it, private victims also seek access to the courts as part of the solution to addressing IP and IT theft, but "civil enforcement alone is insufficient to address the increasingly sophisticated nature and broad scope of IP infringement."[321]

¶111 The real challenge, and opportunity, lies in a partnership between all those involved in public and private enforcement and standard setting. After a review of some of the state, federal, and international enforcement efforts, and a look at the activity of private-sector entities, associations, and individuals, the only truism that seems defensible is that the future of intellectual property rights must involve collaborative and coordinated efforts that span the globe and optimize the use of each entity.[322]

¶112 The recommendation of a massive new partnership is based on the successes, failures, and challenges discussed in this Article. Progress and setbacks are evident at every level, both domestic and international, whether one studies the enforcement actions, accomplishments, and shortcoming of governmental entities, or the efforts of nongovernmental parties and associations. No matter how one assesses each of these efforts to protect IP and IT, there is almost no meaningful collaboration or collective action on behalf of rights holders.

---

[318] *See* Higgins, *supra* note 305, at 170 ("[S]oftware piracy literature has also shown that individuals are likely to perform a behavior when they believe the behavior to be ethical rather than unethical . . . .").

[319] *See* MITCHELL III ET AL., *supra* note 73.

[320] White & Case LLP offered the following suggestions for mitigating the risks of IP theft: "[k]now your supply chain," "[p]rotect yourself contractually," institute policies for "compliance training and awareness building," "[p]ublicize your policy and work with industry groups," and "[t]ake the lead in developing new strategies, rules and best practices." *Id.* at 16–17. A thorough knowledge of the supply chain is essential because "audits alone will not solve the problem" since many companies, often Chinese, hire consultants as plants within companies. *Id.* at 16. Contractual protections can place the burden of risk on the supplier; form the basis for terminating the relationship if violations occur; and provide indemnification if the company is sued by a U.S. plaintiff. *Id.* Publicizing company policies in regulatory filings, publications, and company websites further mitigates these threats. *Id.* at 17. Finally, companies should work together to define industry-wide best practices in monitoring supply chains for unauthorized IP. Because these best practices do not currently exist, business coalitions, national governments, and international organizations should work to implement these necessary measures. *Id.* at 17. *See also* Kappos, *supra* note 62 (discussing how state attorneys general are using unfair competition law to combat international IP theft).

[321] COMPUTER CRIME & INTELLECTUAL PROP. SECTION, DEP'T OF JUSTICE, PROSECUTING INTELLECTUAL PROPERTY CRIMES 4 (4th ed. 2013).

[322] There are a number of international organizations—some mentioned earlier in this Article—that include public and private members and are involved in education, standard setting, and enforcement. Many require all members to report regularly on activities undertaken to achieve the objectives of the group. Some are dedicated to prevention of IP and IT theft. As noted earlier, none have the reach, juridical force, resources, membership, reliable enforcement mechanisms, and other features of a true multidimensional transnational partnership. *See supra* note 1. See also, for example, the International Code of Conduct for Private Security Service Providers (Nov. 9, 2010), *available at* http://www.icoc-psp.org/, which as of September 1, 2013, had 708 signatory companies agreeing to abide by the governance, compliance, and accountability standards defined therein.

¶113 Governments and individuals independently seek solutions—often with great commitment and energy—and yet the impact of IP and IT theft detailed at the start of this Article speaks for itself. There are powerful groups, such as the MPAA,[323] RIAA,[324] and software industry groups,[325] that function independently but are not collaborating on copyright infringement. Similarly, many groups committed to preventing or limiting patent infringement and theft of trade secrets, while having the interests of different stakeholders, share a common overall mission—and yet do not collaborate. To paraphrase Benjamin Franklin,[326] since these groups do not "hang together," they run a fairly high risk of "hanging alone."[327]

V. CONCLUSION

¶114 Partnership allows for widespread buy-in on the basic premise of this work: IP and IT theft exacts an enormous price and suppresses innovation, invention, creativity, and efficiency.

¶115 This premise can be the theme of an ongoing, multinational conference or partnership. That much of IP and IT theft takes place in countries like India and China, as suggested throughout this Article,[328] means that such countries must be included in this effort or it has no hope of succeeding. Partners in such a collaboration could:

(1) Meet and exchange information about successes and challenges in IP and IT protection.

(2) Pledge to enforce fully in courts and agencies the rights of IP and IT owners and report on all enforcement action.

(3) Serve as a standard-setting organization, articulating criteria, proposed statutory and regulatory measures, and best-practice rules.

(4) Report on new in-country rules and standards.

(5) Enforce standards within its membership.

(6) Commit all member governments to enforce IP and IT rights.

(7) Review domestic laws and work to promulgate and implement new standards that facilitate enforcement of IP and IT rights.

(8) Create a worldwide registry and labeling symbology for products and producers that are compliant.

(9) Fund and support educational and other marketing efforts to communicate in every market and in every country the basic ideas regarding the wrongfulness and hazards of IP and IT theft.

(10) Adhere to, internalize, replicate, and enforce "back home" the basic premise above.

---

[323] MOTION PICTURE ASS'N OF AM., http://www.mpaa.org/ (last visited Sept. 5, 2014).

[324] RECORDING INDUS. ASS'N OF AM., http://www.riaa.com/ (last visited Sept. 5, 2014).

[325] *See*, *e.g.*, SOFTWARE & INFO. INDUS. ASS'N, http://www.siia.net/ (last visited Sept. 5, 2014).

[326] *But see The Inquiring Mind*, PUB. BROAD. SERV. (2002), http://www.pbs.org/benfranklin/l3_inquiring_little.html (reporting that Benjamin Franklin did not own patents for his many inventions).

[327] Benjamin Franklin, Remarks at the Continental Congress before the signing of the U.S. Declaration of Independence (July 4, 1776) ("We must, indeed, all hang together, or most assuredly we shall all hang separately.").

[328] *See supra* notes 36–38, 62, 267–269 and accompanying text.

¶116 This partnership will need global reach, substantial resources, and participation by as many as possible of the public and private actors involved in the activity discussed in this Article.

¶117 A partnership of this nature, focused on the above goals, is complex without ready analogue.[329] Membership could include—from every member country—local, state, and federal prosecutors; governmental officials, politicians, and policymakers; representatives of domestic and multinational organizations; representatives of the various executive branches and independent agencies of member governments; corporations; trade associations; academicians; and representatives of interest groups, from authors and software developers to artists, musicians, and select entrepreneurs.

¶118 In this setting, condemnation of IT and IP theft can become part of the social and legal fiber, common and shared, an unquestionable part of the basic and fundamental set of universal governing principles.

[329] Currently, no organizations or initiatives exist that are capable of achieving the goals articulated in this Article. *See*, *e.g.*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/portal/en/ (last visited Sept. 5, 2014); GLOBAL INTELLECTUAL PROP. CTR., U.S. CHAMBER OF COMMERCE, http://www.theglobalip center.com/about/mission-and-goals/ (last visited Sept. 5, 2014); INT'L ASS'N FOR THE PROTECTION OF INTELLECTUAL PROP., https://www.aippi.org/?sel=aims (last visited Sept. 5, 2014); INT'L INTELLECTUAL PROP. INST., http://iipi.org/2010/07/background/ (last visited Sept. 5, 2014); INT'L INTELLECTUAL PROP. ALLIANCE, http://www.iipa.com/ (last visited Sept. 5, 2014); NAT'L CRIME PREVENTION COUNCIL, http://www.ncpc.org/topics/intellectual-property-theft/ncpcs-intellectual-property-theft-campaign (last visited Sept. 5, 2014); Extractive Industries Transparency Initiative, http://eiti.org/eiti (last visited Sept. 5, 2014); FAIR LABOR ASS'N, http://www.fairlabor.org/ (last visited Sept. 5, 2014); International Code of Conduct for Private Security Service Providers, http://www.icoc-psp.org/ (last visited Sept. 5, 2014).