THE IP COMMISSION REPORT

THE REPORT OF
THE COMMISSION ON THE THEFT OF
AMERICAN INTELLECTUAL PROPERTY

THE IP COMMISSION REPORT

THE REPORT OF
THE COMMISSION ON THE THEFT OF
AMERICAN INTELLECTUAL PROPERTY

This report was published on behalf of
The Commission on the Theft of American Intellectual Property
by The National Bureau of Asian Research.

Published May 2013.

Printed in the United States of America.

THE IP COMMISSION REPORT

TABLE OF CONTENTS

ACKNOWLEDGMENTS

We present this report to the American people for their consideration. The Commission on the Theft of American Intellectual Property reached consensus on its insights and recommendations after a thorough and independent investigation of one of the most pressing issues of economic and national security facing our country. We investigated the scale and complexities of international intellectual property (IP) theft, the driving forces behind it, and its consequences for Americans. We collected the evidence, formed assessments, and developed a set of policy recommendations for Congress and the Administration.

This Commission is composed of extraordinary members. We are indebted to our fellow Commissioners for their contributions. They have brought to the Commission diligence, selfless bipartisanship, and tremendous expertise and wisdom. Coming from industry, defense, advanced education, and politics, and with senior-level diplomatic, national security, legal, and other public policy experience, they span the spectrum of American professional life that has huge stakes in IP rights. They have our deepest appreciation.

The Commission reached out to many remarkable specialists and leaders who shared their experiences and perspectives as we developed an understanding of the problem and a very rich set of policy recommendations. Business leaders with whom we spoke provided inputs anonymously; they represent a cross-section of companies that deal with the problem of IP theft, as well as trade associations with major interests in the problem and its solutions. Other interlocutors were officials from Republican and Democratic administrations, policy analysts, lawyers, economists, international trade experts, and international relations and area specialists. We benefited from the efforts of those in the U.S. government who have been working hard on these issues for years. We thank them for their work and hope that our shining the spotlight on the facts and recommending strong policy make their goals more achievable.

The Commission's staff was exemplary. It includes Director Richard Ellings, Deputy Director Roy Kamphausen, Casey Bruner, John Graham, Creigh Agnew, Meredith Miller, Clara Gillispie, Sonia Luthra, Amanda Keverkamp, Deborah Cooper, Karolos Karnikis, Joshua Ziemkowski, and Jonathan Walton. The Commission is grateful to The National Bureau of Asian Research (NBR) and its Slade Gorton International Policy Center, which provided the unrestricted support that underwrote the Commission's work and complete independence.

Leading an effort that attempts to define and prescribe a focus as complex as IP protection is truly daunting. Given the subject of this report, it comes as no surprise that the People's Republic of China figures prominently throughout. It should be noted that we co-chairs have spent a considerable part of our professional lives building and managing important aspects of the U.S.-China relationship. We have participated in and observed the development—whether diplomatic, military, economic, or cultural—of the most critical bilateral relationship of the 21st century, one that will have a significant impact on the security and prosperity of the entire world. Ensuring its viability and success in part gave rise to this Commission and our participation in it. We recognize as well the historic reform efforts that continue to be undertaken in China and offer this report as a step toward solutions and pragmatic problem solving that have characterized the interaction of both countries for over four decades.

Dennis C. Blair
Co-chair

Jon M. Huntsman, Jr.
Co-chair

The Commission on the Theft of American Intellectual Property is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics. The members are:

- **Dennis C. Blair** (co-chair), former Director of National Intelligence and Commander in Chief of the U.S. Pacific Command
- **Jon M. Huntsman, Jr.** (co-chair), former Ambassador to China, Governor of the state of Utah, and Deputy U.S. Trade Representative
- **Craig R. Barrett**, former Chairman and CEO of Intel Corporation
- **Slade Gorton**, former U.S. Senator from the state of Washington, Washington Attorney General, and member of the 9-11 Commission
- **William J. Lynn III**, CEO of DRS Technologies and former Deputy Secretary of Defense
- **Deborah Wince-Smith**, President and CEO of the Council on Competitiveness
- **Michael K. Young**, President of the University of Washington and former Deputy Under Secretary of State

The three purposes of the Commission are to:

1. Document and assess the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States
2. Document and assess the role of China in international intellectual property theft
3. Propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of intellectual property rights by China and other infringers

Introduction

The scale of international theft of American intellectual property (IP) is unprecedented—hundreds of billions of dollars per year, on the order of the size of U.S. exports to Asia. The effects of this theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. Unless current trends are reversed, there is a risk of stifling innovation, with adverse consequences for both developed and still developing countries. The American response to date of hectoring governments and prosecuting individuals has been utterly inadequate to deal with the problem.

China has been the principal focus of U.S. intellectual property rights (IPR) policy for many years. As its economy developed, China built a sophisticated body of law that includes IPR protection. It has a vibrant, although flawed, patent system. For a variety of historical reasons, however, as well as because of economic and commercial practices and official policies aimed to favor Chinese entities

and spur economic growth and technological advancement, China is the world's largest source of IP theft. The evidence presented here is a compilation of the best governmental and private studies undertaken to date, interviews, individual cases, assessments of the impact of IP theft on the American economy, and examinations of PRC policies. There is now enough information, in our view, to warrant urgent consideration of the findings and recommendations that follow.

The IP Commission has met numerous times over the course of an eleven-month period; heard from experts and specialists on international law, the American legal system, cybersecurity, and the economy, as well as from industry representatives and many others; and conducted research on a range of topics. The Commission has also reviewed the current actions being taken by the U.S. government and international organizations like the World Trade Organization (WTO) and the recommendations of official and private studies of the problem. Both current and proposed actions generally emphasize more intensive government-to-government communication requesting foreign governments to rein in their companies and other actors. The Commission judges that the scope of the problem requires stronger action, involving swifter and more stringent penalties for IP theft. The Commission believes that over the long term, as their companies mature and have trade secrets to protect, China and other leading infringers will develop adequate legal regimes to protect the intellectual property of international companies as well as domestic companies. The United States cannot afford to wait for that process, however, and needs to take action in the near term to protect its own economic interests.

The Commissioners unanimously advocate the recommendations contained within this report.

Key Findings

The Impact of International IP Theft on the American Economy

Hundreds of billions of dollars per year. The annual losses are likely to be comparable to the current annual level of U.S. exports to Asia—over $300 billion. The exact figure is unknowable, but private and governmental studies tend to understate the impacts due to inadequacies in data or scope. The members of the Commission agree with the assessment by the Commander of the United States Cyber Command and Director of the National Security Agency, General Keith Alexander, that the ongoing theft of IP is "the greatest transfer of wealth in history."

Millions of jobs. If IP were to receive the same protection overseas that it does here, the American economy would add millions of jobs.

A drag on U.S. GDP growth. Better protection of IP would encourage significantly more R&D investment and economic growth.

Innovation. The incentive to innovate drives productivity growth and the advancements that improve the quality of life. The threat of IP theft diminishes that incentive.

Long Supply Chains Pose a Major Challenge

Stolen IP represents a subsidy to foreign suppliers that do not have to bear the costs of developing or licensing it. In China, where many overseas supply chains extend, even ethical multinational companies frequently procure counterfeit items or items whose manufacture benefits from stolen IP, including proprietary business processes, counterfeited machine tools, pirated software, etc.

International IP Theft Is Not Just a Problem in China

Russia, India, and other countries constitute important actors in a worldwide challenge. Many issues are the same: poor legal environments for IPR, protectionist industrial policies, and a sense that IP theft is justified by a playing field that benefits developed countries.

The Role of China

Between 50% and 80% of the problem. The major studies range in their estimates of China's share of international IP theft; many are roughly 70%, but in specific industries we see a broader range.

The evidence. Evidence comes from disparate sources: the portion of court cases in which China is the destination for stolen IP, reports by the U.S. Trade Representative, studies from specialized firms and industry groups, and studies sponsored by the U.S. government.

Why does China stand out? A core component of China's successful growth strategy is acquiring science and technology. It does this in part by legal means—imports, foreign domestic investment, licensing, and joint ventures—but also by means that are illegal. National industrial policy goals in China encourage IP theft, and an extraordinary number of Chinese in business and government entities are engaged in this practice. There are also weaknesses and biases in the legal and patent systems that lessen the protection of foreign IP. In addition, other policies weaken IPR, from mandating technology standards that favor domestic suppliers to leveraging access to the Chinese market for foreign companies' technologies.

Existing Remedies Are Not Keeping Up

Short product life cycles. Even in the best judicial systems, the slow pace of legal remedies for IP infringement does not meet the needs of companies whose products have rapid product life and profit cycles.

Inadequate institutional capacity. Particularly in developing countries there is inadequate institutional capacity to handle IP-infringement cases—for example, a shortage of trained judges.

China's approach to IPR is evolving too slowly. The improvements over the years have not produced meaningful protection for American IP, nor is there evidence that substantial improvement is imminent. Indeed, cyberattacks are increasing.

Limitations in trade agreements. Although there appears to be a great deal of activity on the part of the United States through the WTO, there are also significant problems in the process that have made it impossible to obtain effective resolutions. Bilateral and regional free trade agreements are not a panacea either.

Steps undertaken by Congress and the administration are inadequate. Actions have been taken recently both to elevate the problem as a policy priority and to tighten U.S. economic espionage law. These are positive steps. A bill in Congress that would allow greater information-sharing between government and private business needs to be enacted and amended if needed. All of these efforts, however, will not change the underlying incentive structure for IP thieves and will therefore have limited effect.

The Commission's Strategy

With U.S. companies suffering losses and American workers losing jobs, and our innovative economy and security thus at stake, more effective measures are required. The problem is compounded

by newer methods of stealing IP, including cyber methods. Of the cyber threat, President Obama has said that it is "one of the most serious economic and national security challenges we face." Network attacks, together with other forms of IP attacks, are doing great damage to the United States, and constitute an issue of the first order in U.S.-China relations.

The Commission regards changing the incentive structure for IP thieves to be a paramount goal in reducing the scale and scope of IP theft. Simply put, the conditions that encourage foreign companies to steal American intellectual property must be changed in large part by making theft unprofitable. The starting point is the recognition that access to the American market is the single most important goal of foreign firms seeking to be international corporate leaders. Companies that seek access by using stolen intellectual property have an unearned competitive advantage, and because the costs of stealing are negligible or nonexistent, they continue to operate with impunity. Cheating has become commonplace.

The Commission regards changing the cost-benefit calculus for foreign entities that steal American intellectual property to be its principal policy focus. IP theft needs to have consequences, with costs sufficiently high that state and corporate behavior and attitudes that support such theft are fundamentally changed.

Beyond changing behavior in the short term, the Commission regards strengthening the legal frameworks that govern the protection of IP to be a set of important medium-term recommendations. From that point, and over the longer term, the Commission judges that capacity-building in countries, especially China, that have poor IP-protection standards is of critical importance.

Recommendations

The Commission recommends short-term, medium-term, and long-term remedies.

Short-term measures incorporate the immediate steps that policymakers should take to stem the tide of IP theft and include the following:

- *Designate the national security advisor as the principal policy coordinator for all actions on the protection of American IP.* The theft of American IP poses enormous challenges to national security and the welfare of the nation. These challenges require the direct involvement of the president's principal advisor on national security issues to ensure that they receive the proper priority and the full engagement of the U.S. government.
- *Provide statutory responsibility and authority to the secretary of commerce to serve as the principal official to manage all aspects of IP protection.* The secretary of commerce has sufficient human, budgetary, and investigative resources to address the full range of IP-protection issues. If given the statutory authority to protect American IP, we anticipate a robust set of responses.
- *Strengthen the International Trade Commission's 337 process to sequester goods containing stolen IP.* The current 337 process is not fast enough to prevent goods containing or benefitting from stolen IP from entering the United States. A speedier process, managed by a strong interagency group led by the secretary of commerce, can both prevent counterfeit goods from entering the United States and serve as a deterrent to future offenders. The speedier process would impound imports suspected of containing or benefitting from IP theft based

on probable cause. A subsequent investigation would allow the importing company to prove that the goods did not contain or benefit from stolen IP.

- *Empower the secretary of the treasury, on the recommendation of the secretary of commerce, to deny the use of the American banking system to foreign companies that repeatedly use or benefit from the theft of American IP.* Access to the American market is a principal interest of firms desiring to become global industrial leaders. Protecting American IP should be a precondition for operating in the American market. Failure to do so ought to result in sanctions on bank activities, essentially curtailing U.S. operations.
- *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.* The increase in trade-secret theft, in many ways enabled by emerging cyber capabilities, requires a significant increase in investigative and prosecutorial resources.
- *Consider the degree of protection afforded to American companies' IP a criterion for approving major foreign investments in the United States under the Committee on Foreign Investment in the U.S. (CFIUS) process.* CFIUS assesses national security risk and national security implications of proposed transactions involving U.S. companies. Adding an additional evaluative criterion to the review process that assesses the manner in which a foreign company obtains IP would help improve IP-protection environments.
- *Enforce strict supply-chain accountability for the U.S. government.* Establishing control and auditing measures that enable suppliers to the U.S. government to guarantee the strongest IP-protection standards should be the "new normal" that the U.S. government demands.
- *Require the Securities and Exchange Commission to judge whether companies' use of stolen IP is a material condition that ought to be publicly reported.* Corporate leaders will take seriously the protection of IP, including in their supply chains, if reporting IP theft in disclosure statements and reports to boards of directors and shareholders is mandatory.
- *Greatly expand the number of green cards available to foreign students who earn science, technology, engineering, and mathematics degrees in American universities and who have a job offer in their field upon graduation.* In too many cases, American universities train the best minds of foreign countries, who then return home with a great deal of IP knowledge and use it to compete with American companies. Many of these graduates have job offers and would gladly stay in the United States if afforded the opportunity.

Legislative and legal reforms represent actions that aim to have positive effects over the medium-term. To build a more sustainable legal framework to protect American IP, Congress and the administration should take the following actions:

- *Amend the Economic Espionage Act (EEA) to provide a federal private right of action for trade-secret theft.* If companies or individuals can sue for damages due to the theft of IP, especially trade secrets, this will both punish bad behavior and deter future theft.
- *Make the Court of Appeals for the Federal Circuit (CAFC) the appellate court for all actions under the EEA.* The CAFC is the appellate court for all International Trade Commission cases and has accumulated the most expertise of any appellate court on IP issues. It is thus in the best position to serve as the appellate court for all matters under the EEA.

- *Instruct the Federal Trade Commission (FTC) to obtain meaningful sanctions against foreign companies using stolen IP.* Having demonstrated that foreign companies have stolen IP, the FTC can take sanctions against those companies.
- *Strengthen American diplomatic priorities in the protection of American IP.* American ambassadors ought to be assessed on protecting intellectual property, as they are now assessed on promoting trade and exports. Raising the rank of IP attachés in countries in which theft is the most serious enhances their ability to protect American IP.

Over the longer term, the Commission recommends the following capacity-building measures:

- *Build institutions in priority countries that contribute toward a "rule of law" environment in ways that protect IP.* Legal and judicial exchanges, as well as training programs sponsored by elements of the U.S. government—including the U.S. Patent and Trademark Office—will pay long-term dividends in the protection of 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. New technologies, either to validate the integrity of goods or to detect fraud, would both deter bad behavior and serve as models for the creation of new IP.
- *Ensure that top U.S. officials from all agencies push to move China, in particular, beyond a policy of indigenous innovation toward becoming a self-innovating economy.* China's various industrial policies, including indigenous innovation, serve to dampen the country's own technological advancements. Utility, or "petty," patents are a particularly pernicious form of Chinese IP behavior and need to cease being abused.
- *Develop IP "centers of excellence" on a regional basis within China and other priority countries.* This policy aims to show local and provincial leaders that protecting IP can enhance inward foreign investment; this policy both strengthens the protection of IP and benefits the promotion possibilities of officials whose economic goals are achieved by producing foreign investment.
- *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.* One of the tools necessary to develop "centers of excellence" is a rating system that shows the best—and worst—geographical areas for the protection of IP.

The Commission recommends the following measures to address cybersecurity:

- *Implement prudent vulnerability-mitigation measures.* This recommendation provides a summary of the security activities that ought to be undertaken by companies. Activities such as network surveillance, sequestering of critical information, and the use of redundant firewalls are proven and effective vulnerability-mitigation measures.
- *Support American companies and technology that can both identify and recover IP stolen through cyber means.* Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information.

- *Reconcile necessary changes in the law with a changing technical environment.* Both technology and law must be developed to implement a range of more aggressive measures that identify and penalize illegal intruders into proprietary networks, but do not cause damage to third parties. Only when the danger of hacking into a company's network and exfiltrating trade secrets exceeds the rewards will such theft be reduced from a threat to a nuisance.

Chapter 1

The Nature of the Problem

Economic Development in the Postwar Period

The unprecedented economic growth in country after country since the Second World War followed a familiar pattern. Taking advantage of reduced barriers to international trade and their lower costs for labor and other expenses, less developed countries manufactured lower-technology products and provided lower-technology services for sale to the more developed countries. The developed countries, meanwhile, closed entire industries and converted their labor forces to work on more advanced products and services based on newly invented products and processes. Prosperity increased as new technologies drove productivity gains and wages rose. Countries moved up the technology ladder.

This system produced phenomenal benefits for both the developed and developing worlds, and generations had the chance to live better lives than their parents and grandparents. In the period since the Second World War, humanity experienced more economic growth, which was led by more scientific progress, than at any prior time in history. From 1950 to 2012, world output expanded more than sixteen-fold, while population grew 2.7 times.[1] Driven by scientific breakthroughs, new technologies, and open trade, standards of living and life expectancy skyrocketed for enormous populations worldwide.[2]

This virtuous cycle of innovation, with benefits for both developed and developing countries, depended on innovators receiving adequate compensation for the risks they took. The developing world acquired and adapted foreign technology, but the driving discoveries in the areas of information technology, materials science, and biochemistry came from a combination of entrepreneurship and private and government research in the developed world—primarily the United States, Western Europe, and Japan. These discoveries gave birth to entire new manufacturing and service industries and transformed traditional sectors like transportation and health care.

The Underpinnings of an Economic System at Risk

On an unprecedented level, a critical driver of this worldwide economic growth is in trouble. Trade secrets, patents, copyrights, and trademarks are being stolen, especially from American but also from European, Japanese, and other nations' companies and organizations. The effects are twofold. The first is the loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them. In addition, there is the loss of jobs, which is in the millions. Companies injured by the theft of intellectual property (IP) cut back

[1] See Angus Maddison, *The World Economy: A Millennial Perspective/Historical Statistics* (Paris: OECD, 2007); and International Monetary Fund (IMF) and World Bank statistics. From the year 1000 to 1820 the advance in per capita income was "a slow crawl"—the world per capita income rose only about 50% in 820 years. Most of the growth went to accommodate a fourfold increase in population. From about 1820, world development began accelerating far faster than population growth. Between 1820 and 1950 the world economy grew nearly eightfold. In less than half that time, between 1950 and 2012, the world economy grew more than sixteen-fold. Figures are measured in constant dollars.

[2] See, for example, the Human Development Index, published annually by the United Nations Development Programme. Drawing on data that goes back to 1975, the index shows gains in human development in all regions of the world. Even the industrialized world shows marked improvements. In the United States, average life expectancy at birth has grown for all groups by 10%–15% since 1949.

on payrolls. Payrolls are also hit by lost export and licensing markets and unfair competition both in the American market and in markets around the world. The losses are more acute for companies whose innovation cycles are ever shorter. IP theft prior to or soon after a product's release can eliminate all or vast portions of what a company could earn.

The second, and more fundamental, effect is that IP theft is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and new industries that can further expand the world economy and continue to raise the prosperity of all. This effect has received some attention in the cases of a few industries, but it affects others as well. Unless current trends are reversed, there is a risk of the relative stagnation of innovation, with adverse consequences for both developed and developing countries.

Because IP theft is not a new phenomenon, it is important to understand why it is an urgent issue now. Compared with prior eras, today's economic world is far more interconnected and operates at a far higher speed, with product cycles measured in months rather than years. Companies in the developing world that steal intellectual property from those in the developed world become instant international competitors without becoming innovators themselves. Bypassing the difficult work of developing over decades the human talent, the business processes, and the incentive systems to become innovators, these companies simply drive more inventive companies in the developed world out of markets or out of business entirely. If more and more companies compete for the same amount of business using the same technology and processes, growth stagnates. It is only through innovation that world economic growth can be sustained. In addition, in this new era of globalization, national industrial policies unforeseen in times past have become possible. Many countries have taken advantage of the opportunities provided by international businesses eager for entry into their markets and by generous national and international development programs. Some have gone beyond this by leveraging access to their markets for IP and by sponsoring IP theft.

Finally, the enormous scale of IP theft is a relatively recent phenomenon, and the United States and the rest of the developed world have been slow to respond. American policy in this area has been limited mostly to attempts to talk foreign leaders into building more effective intellectual property rights (IPR) regimes. In addition, the U.S. Department of Justice has prosecuted individual employees of American companies who have been caught attempting to carry trade secrets with them to foreign companies and entities. This policy of jawboning and jailing a few individuals has produced no measurable effect on the problem. The only encouraging sign on the horizon is a nascent and small group of entrepreneurs who may be working within their developing countries for more robust systems of protection of their own inventions against competitors.

If the United States continues on its current path, with the incentives eroding, innovation will decline and our economy will stagnate. In this fundamental sense, IP theft is now a national security issue.

The theft of American IP is about much more than the aggregation of big numbers. It is also the collection of individual, sometimes devastating, stories of loss. For instance, when the American Superconductor Corporation had its wind-energy software code stolen by a major customer in China, it lost not only that customer, but also 90% of its stock value.

SOURCE: Michael A. Riley and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies," *Bloomberg Businessweek*, March 19–25, 2012.

The Toll of IP Theft and Vulnerable Supply Chains

It is difficult to overstate the importance of intellectual property to U.S. economic prosperity and difficult to gauge the full extent of the damage done by IP theft. According to a figure cited in the president's 2006 Economic Report to Congress, 70% of the value of publicly traded corporations is estimated to be in "intangible assets," that is, IP. A 2012 study by the Department of Commerce found that protection and enforcement of IPR around the globe directly affects an estimated 27 million American jobs in IP-intensive industries, which is roughly 19% of the U.S. workforce, producing over one-third of America's GDP. [3]

Overseas, products are counterfeited on a mammoth scale or re-engineered with small changes and then patented as if they were new inventions. Because much of the theft is not counted, estimates of the total vary. In 2010, the commander of the U.S. Cyber Command and director of the National Security Agency, General Keith Alexander, stated that "our intellectual property here is about $5 trillion. Of that, approximately $300 billion [6%] is stolen over the networks per year." [4] He later called the theft "the greatest transfer of wealth in history."[5]

Intellectual property that is stolen over the Internet constitutes only a portion of total IP theft. Much of it occurs the old-fashioned way. Hard drives are either duplicated on site or physically stolen by bribed employees; employees are planted temporarily in companies or permanent employees leave and illegally share proprietary information; products are dissected, re-engineered, and sold without permission or payment of royalties; digitized products are pirated and sold illegally; phones are tapped for the purpose of obtaining trade secrets; and email accounts are compromised. The list goes on. The stories that appear in court records and occasionally appear in the media demonstrate that while there are new tools being utilized in IP theft, traditional tools continue to cause enormous damage. *Totaled, it is safe to say that dollar losses from IP theft are hundreds of billions per year,* which is at least in the range of total exports to Asia in 2012 (valued at $320 billion).

Indeed, IP is hugely important to the U.S. economy. Loss of revenues to the victimized inventor or owner of a trade secret is the first and most obvious cost of IP theft, but an asset is lost too. Both losses mean fewer jobs and less money to reinvest in the next generation of products. Stolen IP represents a subsidy to the party that did not have to bear the costs of developing it, and the effects can ripple across industries and companies. A prime example is the pirated software utilized in manufacturing systems and management of companies. Stolen corporate software—from basic computer and network operating systems and office technology to sophisticated design algorithms—allows companies to cut costs unfairly. The problem is rampant in many countries around the world, but in the People's Republic of China (PRC), a country to which so many overseas supply chains extend, even ethical multinational companies find themselves complicit.

The member companies of the American Chamber of Commerce in the People's Republic of China (AmCham China) express their concerns in annual surveys. In the most recent, conducted in late 2012, over 40% of respondents reported that the risk of data breach to their operations in China

---

[3] U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012.

[4] Jim Garamone, "Cybercom Chief Details Cyberspace Defense," American Forces Press Service, September 23, 2010. A decade ago the U.S. government reported that "private estimates put the combined costs of foreign and domestic economic espionage [by all methods], including the theft of intellectual property, as high as $300 billion per year and rising." See "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002," Office of the National Counterintelligence Executive, NCIX 2003-10006, 2003.

[5] Keith B. Alexander, "Cybersecurity and American Power" (conference presentation hosted by the American Enterprise Institute, Washington, D.C., July 9, 2012).

is increasing, and those who indicated that IP infringement has resulted in "material damage" to China operations or global operations increased from 18% in 2010 to 48% in 2012.[6]

The longer the supply line, the more vulnerable it is to IP theft. In an extensive study of the Department of Defense's supply chain, the U.S. Senate Armed Services Committee reported a "flood" of counterfeit parts. The investigation

> uncovered 1,800 cases of suspect electronic parts. The total number of individual suspect parts involved in those cases exceeded one million.
>
> China is the dominant source country for counterfeit electronic parts that are infiltrating the defense supply chain..... The Committee tracked well over 100 cases of suspect counterfeit parts back through the supply chain. China was found to be the source country for suspect counterfeit parts in an overwhelming majority of those cases, with more than 70 percent of the suspect parts traced to that country.[7]

One of the witnesses in the investigation testified that he observed "factories in China of 10,000 to 15,000 people set up for the purpose of counterfeiting." Electronic components can be compromised both unintentionally and intentionally and could be subject to embargoes in times of crisis. Fierce competition gives the cheating overseas supplier a cost advantage, but at the expense of American firms, American employees, American security, and future American innovation.

A 2011 study by the U.S. International Trade Commission estimated that if IP protection in just China were improved to a level comparable to that in the United States, the U.S. economy would obtain an estimated $107 billion in additional annual sales and net U.S. employment could increase by 2.1-million jobs.[8] Yet as useful as it is, this study underestimated employment impacts because it did not consider "less-IP intensive industries," likely underestimated the effects of trade-secret theft (much of which is never revealed or even known by the victims), and did not have the participation of many vulnerable U.S. companies.[9]

Despite the understandable reluctance of companies to publicize successful or even attempted breeches, there are many documented examples of IP theft. An American company, for example, developed at great cost a critical component in current smartphones and computers, only to have that technology illegally replicated by a Chinese company. The latter subsequently undersold the inventor and took much of the world market for the technology. In another case, one copy of an American company's software was purchased in China and illegally copied onto 30 million Chinese

---

6 "American Chamber's Business Climate Survey 2013," China IPR web log, April 22, 2013, http://chinaipr.com/2013/04/22/american-chambers-business-climate-survey-2013/; American Chamber of Commerce, "China Business Climate Survey Report," 2011, http://www.amchamchina.org/upload/cmsfile/2011/03/22/efb2ab9d3806269fc343f640cb33baf9.pdf; and American Chamber of Commerce, "China Business Climate Survey Report," 2013, http://web.resource.amchamchina.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf.

7 U.S. Senate Committee on Armed Services, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 112th Cong., 2nd sess., Report 112-167, May 21, 2012.

8 U.S. International Trade Commission (USITC), *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, xviii–xx, http://www.usitc.gov/publications/332/pub4226.pdf. In addition, an estimate of the international value during 2009–15 of just pirated and counterfeited goods, such as software and clothing, is $1.12 trillion. See Pamela Passman, "How to Protect Intellectual Property: From Fair Trade to Legal Trade," *Foreign Affairs*, February 27, 2013.

9 Nor do these findings take into account that IP theft also increases cybercrime and other security threats, particularly with regard to counterfeit software use. According to a recent report by the International Data Corporation (IDC), counterfeit software is a major vehicle for carrying dangerous malware that imposes costs on the economy and exposes IT systems and data. The IDC study states that "the direct costs to enterprises from dealing with malware from counterfeit software will hit $114 billion" in 2013 and "potential losses from data breaches could reach nearly $350 billion." See John F. Gantz et al., "The Dangerous World of Counterfeit and Pirated Software: How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations … and the Resultant Costs in Time and Money," IDC, White Paper, no. 239751, March 2013, 3–4, http://www.computerworld.com.pt/media/2013/03/IDC030513.pdf.

computers, an act of piracy with a multibillion dollar commercial value.[10] While most cases of IP theft do not end up in courts, twenty trade-secret cases involving China revealed the wide range of industries hit: automobiles, automobile tires, aviation, chemicals, consumer electronics, defense systems, electronic trading, industrial software, and pharmaceuticals.[11]

American scientific innovations and new technologies are tracked and stolen from American universities, national laboratories, private think tanks, and start-up companies, as well as from the major R&D centers of multinational companies. Virtually every sector and technology is attacked—from low-tech to high-tech; from agricultural machinery and biotechnology to wind-power generation; from mobile phones, computers, and televisions to chemical compounds and aeronautics.

Start-up companies are at the heart of the American innovative society. In his 2012 State of the Union address, President Obama noted the important place of start-ups when he observed that "innovation is what America has always been about. Most new jobs are created in start-ups and small businesses."[12]

Start-ups rely heavily on IP protection just to get their inventions to market. As the Biotechnology Industry Organization (BIO) points out, "the vast majority of BIO's members are small and medium sized enterprises that currently do not have products on the market. As such BIO's members rely heavily on the strength and scope of their patents to generate investment to take their technologies to commercialization."[13] Start-ups, such as those in the biotech field, are extremely vulnerable to IP theft. Typically located in "incubator" areas near major research universities, these small operations have limited legal and technological resources to deal with the nearly relentless efforts targeting their IP. Moreover, they are often staffed by graduate students or post-degree fellows, who sometimes turn into "walking IP" and take trade secrets with them when they leave. As BIO observes, once the IP is lost, the company may simply fold because it is unable to attract any investment.

In addition to the illegal forms of IP theft, the United States may be losing a significant portion of its IP through completely legal and even institutionalized means. For example, each year hundreds thousands of students from all over the world come to the United States to pursue science, technology, engineering, and mathematics graduate degrees. Upon graduation, many return to their country of origin, not because they choose to but because current U.S. immigration law limits the number of visas granted to these graduates. This cap on visas forces thousands of highly skilled workers, a core input for economic growth and production, to leave the country, taking their knowledge, skills, and innovative spirit with them.

[10] Leo Hindery Jr., "China's Latest Target in Its Trade War Against American Manufacturing: The U.S. Solar Industry," Huffington Post, March 6, 2012, http://www.huffingtonpost.com/leo-hindery-jr/china-solar-panels-_b_1323568.html.

[11] Michael A. Riley and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind Out of U.S. Companies," *Businessweek*, March 15, 2012; and Ann Woolner et al., "The Great Brain Robbery," *Businessweek*, March 15, 2012.

[12] "Remarks by the President in State of the Union Address," White House, Office of the Press Secretary, January 24, 2012, http://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address.

[13] Stanford McCoy, "Biotechnology Industry Organization: 2013 Special 301 Submission," Biotechnology Industry Organization, 2013, http://www.bio.org/sites/default/files/2013%20BIO%20Submission.pdf.

Weak Rule of Law and the Absence of a Culture of Compliance

Contributing to the problem of IP theft globally is a lack of institutional capacity and a general unwillingness to confront the issue at a national level. Often, judicial resources are either not utilized or lack the capacity or experience to hear cases. Likewise, there is a lack of criminal sanctions for end-users in some countries where IPR violations are rife. The two most populous nations in the world, India and China, suffer from inefficient judicial institutions, have weak criminal enforcement of IPR violations, and seldom impose sentences that would rise to the level of deterrence for IP crimes. In China, for example, the courts are overwhelmed with cases, and judges in the IP courts are spread thinly.[14] Barriers to discovery in China also remain a vexing problem for U.S. parties seeking redress both there and in U.S. courts.[15] Despite improvements in some sectors following China's 2010 Special IPR Enforcement Campaign, the country remained on the "priority watch list" published by the United States Trade Representative (USTR) in 2012 and 2013. The USTR notes that IP protection and enforcement remain a significant challenge.[16]

Even where there are established administrative mechanisms to deal with IPR protection, such mechanisms often suffer from understaffing, underfunding, bureaucratic paralysis, or a combination of hindrances. As an example, a confluence of factors limits the effectiveness of China's copyright bureaucracy. Devolution of state power to the local level, local protectionism, lack of sufficient resources, and low bureaucratic rank have all been cited as reasons for the inefficacy of the National Copyright Administration and its local counterparts.[17]

Further, China has just redrafted its Guidelines on Anti-Monopoly Enforcement for Intellectual Property, and certain provisions could possibly be used to penalize IP producers rather than spur innovative activity. For instance, the guidelines require compulsory licensing of IP when a company is deemed to be in a dominant market position. In a disconcerting trend that has emerged in recent court cases, patent holders have been forced into compulsory licenses for their patents at rates that are far below market value (e.g., in *Interdigital v. Huawei*), and the definition of what constitutes a "dominant market position" remains unclear.[18] While establishing guidelines for anti-monopoly enforcement of IP and opening these rules up for public comment are positive steps, more must be done to ensure that these guidelines are not used to suppress innovative activity rather than encourage it.

What Countries?

The USTR's 2013 Special 301 Report reviews the state of IPR protection and enforcement across the globe. In its most recent report on U.S. trading partners, the USTR identifies 1 priority country (Ukraine), while including 10 countries on its "priority watch list" and 30 on its "watch list." Most of these 41 countries are the subject of a sternly worded paragraph on problems in their IPR protection

---

[14] Interview with a senior judge in the No. 2 Intermediate People's Court, IP Division, 2010.

[15] See Allison Walton and Dean Gonsowski, "Like the Great Wall: E-discovery Barriers Still Exist between the U.S. and China," *Inside Counsel*, December 3, 2012, http://www.insidecounsel.com/2012/12/03/like-the-great-wall-e-discovery-barriers-still-exi.

[16] Office of the U.S. Trade Representative (USTR), "2012 Special 301 Report," April 2012, http://www.ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf; and Office of the USTR, "2013 Special 301 Report," May 2013, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

[17] As Andrew Mertha notes, the state is not necessarily complicit in the devolution of power; rather, it may actually objectively recognize the limitations of its own abilities to control certain activities at the local level. See Andrew C. Mertha, *China's Water Warriors: Citizen Action and Policy Change* (Ithaca: Cornell University Press, 2008), 159.

[18] See Frank Schoneveld, "Abuse of IP Rights under China's Antitrust Rules: Recent Cases Have a Potentially Serious Impact," Lexology, March 22, 2013, http://www.lexology.com/library/detail.aspx?g=9f45d667-7444-4a74-ae61-bf4b5d04e0fe.

and enforcement. Beyond the special focus on Ukraine, however, 3 countries on the priority watch list warrant more extensive comments: India, Russia, and China.

According to the USTR, the outlook for Indian protection of IP is discouraging, so much so that "there are serious questions about the future condition of the innovation climate across multiple sectors and disciplines." Companies, for example, are challenged to patent and defend already patented pharmaceuticals. If a recent case serves as a precedent, companies from many sectors may be forced into compulsory licensing if they wish to sell in the country but do not manufacture the product there.

Russia frequently ranks among the worst-offending countries in the USTR's Special 301 reports, and this year's assessment finds an overall decline in IPR enforcement. However, with Russia's accession to the WTO, some improvement in the piracy rate of software, and the introduction of a new special court, the report is hopeful about the future.

China receives the lion's share of attention in the 2013 report, which notes that according to the U.S. National Counterintelligence Executive, "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The USTR also cites evidence from privately sponsored studies suggesting that entities "affiliated with the Chinese military and Chinese Government" have obtained "all forms of trade secrets." Overall, the report describes Chinese companies and entities as "escalating" infringement of trade secrets and continuing infringement of trademarks, copyrights, and patents. In addition, it notes that "central, provincial, and local level Chinese agencies inappropriately require or pressure rights holders to transfer IPR from foreign to domestic entities."[19]

The indicators of China's complex role in IPR infringement come from a host of other studies over the years. Of the counterfeit or pirated goods seized by U.S. Customs and Border Protection in 2012, 72% were Chinese in origin.[20] Seven of the eleven cases brought under the Economic Espionage Act since 2010 concern stolen IP destined for Chinese entities. For almost all categories of IP theft, currently available evidence and studies suggest that between 50% and 80% of the problem, both globally and in the United States, can be traced back to China.

By legal as well as illegal means, China has done a Herculean job of absorbing American and other countries' technology. China now manufactures more cars than any other country, in 2012 producing almost as many as the United States and Japan combined;[21] launches astronauts into orbit; assembles and makes many components for sophisticated consumer products like the iPad; leads the world in many green industries; builds most of the world's new nuclear power plants; is rapidly advancing its military technology, often at a quicker pace than most experts predict; and makes some of the world's fastest supercomputers. China is projected to pass the United States in total economic output between 2016 and 2030, depending on the source and methodology used.[22] At the point of GDP parity, each of the two economies will account for an estimated 18% of world product.

Beyond these accomplishments, which suggest extraordinary inputs, are factors that make China the biggest IP offender in the world. In the first major study on China and IPR, Michel Oksenberg

---

19 See USTR, "2013 Special 301 Report," especially 13, 31–38.

20 U.S. Customs and Border Protection, "Intellectual Property Rights: Fiscal Year 2012 Seizure Statistics," Office of International Trade, 0172-0113, January 17, 2013.

21 Patrick Blain (presentation at the 2013 Geneva Motor Show OICA Press Conference, Geneva, March 6, 2013), 10, http://oica.net/wp-content/uploads/pc-oica-geneve-2013-v3b.pdf.

22 These projections from the IMF's 2011 "World Economic Outlook" are based on PPP measurements; see also the 2030 projection from the World Bank.

and colleagues noted in 1996 that the problem in China begins with historical and cultural factors, which are then exacerbated by leadership priorities, bureaucracies competing for authority, an immature legal system, and local-level leaders motivated first and foremost by short-term economic and political interests. "This widespread disregard for intellectual property rights," they wrote, "is an area of great concern for all high-technology firms operating in the Chinese market…. and won't be easily solved."[23]

Nearly two decades later, IPR still suffers from lax enforcement by a judicial system that, despite extraordinary reforms, does not deter IP theft. In fact, the most recent member surveys by AmCham China suggest that the situation is deteriorating. In 2012 the percentage of responding companies that classified IPR enforcement as "ineffective" and "totally ineffective" rose to 72%.[24] Doing business in China entails navigating a system that defies the outsider's full apprehension, and IP theft represents a special risk.[25]

PRC Policy

The legacy of the "four modernizations" policy, launched by Deng Xiaoping in 1978, is crucial to understanding IPR in China. The targets of Deng's remarkably successful development policy were the core economic sectors of society, and foreign IP was seen as crucial for each. The Chinese government elicited the support of the UN Development Programme in fall 1978 for technical assistance and financial resources. China soon became the World Bank's major recipient of support. To accelerate the modernization process, foreign trade was encouraged, with machinery and know-how from the West and Japan purchased or obtained through aid or other means. Eventually millions of Chinese studied abroad, many of them in the sciences. Having adopted fundamental reforms that included an export-led growth strategy similar to those that were pioneered by Japan and the "four tigers," China was able to speed up its economic development with foreign investment and access to technologies and management expertise.[26]

Over the years, the policy to acquire and develop technology has existed under different names and been given subtly different emphases. U.S. firms and national labs were targeted from the beginning. A congressional report documented successful efforts between the late 1970s and mid-1990s by a range of Chinese actors to obtain very advanced technologies.[27] By the late 1980s, American companies and trade negotiators were complaining, as reflected in the USTR Special 301 reports. These reports serve as an instructive historical record from 1989 to the present. The very first report listed China as one of the top three IPR offenders, and by 1996 China stood alone as the country of greatest concern.

At the core of the "indigenous innovation" policy launched in 2006 and incorporated into the National Medium- and Long-Term Plan for the Development of Science and Technology (2006–2020) were procurement rules that further favored Chinese companies, advantages for Chinese companies

---

23 Michel Oksenberg, Pitman B. Potter, and William B. Abnett, "Advancing Intellectual Property Rights: Information Technologies and the Course of Economic Development in China," *NBR Analysis* 7, no. 4 (1996): 1–35.

24 American Chamber of Commerce, "China Business Climate Survey Report," 2013.

25 For a practical view by an American business lawyer and China hand, see Dan Harris, "How to Protect Your IP from China," China Law Blog, parts 1–5, October 4–11, 2012, http://www.chinalawblog.com/2012/10/how-to-protect-your-ip-from-china-part-5.html.

26 The four tigers of Asia are Hong Kong, the Republic of Korea, Singapore, and Taiwan.

27 Christopher Cox, "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," Select Committee, United States House of Representatives, May 1999, http://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf; and Justin Schenk and Evan Perez, "FBI Traces Trail of Spy Ring to China," *Wall Street Journal*, March 10, 2012, http://online.wsj.com/article/SB10001424052970203961204577266892884130620.html.

in the protection of IP and in the patent system,[28] efforts to set Chinese technology standards to favor Chinese entities, requirements for foreign companies to share or expose their technologies for access to the Chinese market, and subsidies for key industries to enable them to beat foreign competitors. Many foreign businesses came to see the heightened mandate to import technologies and assimilate them as justification for greater theft of foreign-generated IP, as well as for stronger pressure on foreign companies to share technology. An increase in theft and compulsory technology transfer in fact seems to have been the outcome.[29] China's indigenous innovation policy also included a mandate to consolidate industry so that one or a few Chinese companies would dominate key sectors. After decades of reforms, state-owned enterprises today produce an estimated half of China's total manufacturing and services output, and they dominate such sectors as energy, telecommunications, and transportation.[30]

In China's 12th five-year plan (2011–15), developing technological capabilities across a broad swath of industries remains a top priority. Added to the plan in July 2012 were seven "national strategic emerging industries" of special interest, on top of the traditional focuses. These seven industries are (1) *new energy auto industry*, (2) *energy-saving and environmental-protection industry* (energy-efficient industry, advanced environmental-protection industry, resource-recycling industry), (3) *new-generation information-technology industry* (next-generation information-network industry, fundamental industry of core electronics, high-end software, and new information-service industry), (4) *biotechnology industry* (bio-pharmaceutical industry, bio-medical engineering industry, bio-breeding industry, bio-manufacturing industry), (5) *high-end equipment manufacturing industry* (aviation equipment industry, satellite and satellite application industry, rail transportation equipment industry, marine engineering equipment industry, intelligent equipment-manufacturing industry), (6) *new energy industry* (nuclear energy technology industry, wind energy industry, solar energy industry, biomass industry), and (7) *new material industry* (new functional-material industry, advanced structural-material industry, high-performance composite-material industry).

As the new Chinese leadership settles in, IPR issues loom. The fundamental question is whether the new leaders will confront the major societal and policy forces that continue to work against IPR. The patent and trade-secret legal environments, for example, require reform. The patent system encourages Chinese entities to copy and file foreign patents as if these patents were their own, and seems to establish the right of Chinese entities to sue the foreign, original inventor that seeks to sell the technology in China. A deluge of such suits could occur in the next few years. Separately, proposed legal amendments are now circulating that would force foreign companies into licensing agreements in exchange for those companies' access to the Chinese market. The amendments would produce a situation similar to the one developing in India, where foreign manufacturers may be prevented from importing their products and left with the choice of either licensing their technology to an Indian firm or manufacturing products in the country if they wish access to the Indian market.

---

[28] For example, the PRC pays entities to file for patents, and most patents are granted based on small or no design changes from the foreign originals.

[29] James McGregor, "China's Drive for 'Indigenous Innovation'—A Web of Industrial Policies," U.S. Chamber of Commerce, July 28, 2010, http://www.uschamber.com/sites/default/files/reports/100728chinareport_0.pdf.

[30] Andrew Szamosszegi and Cole Kyle, "An Analysis of State-owned Enterprise and State Capitalism in China," prepared for the U.S.-China Economic and Security Review Commission, October 26, 2011, 1, http://origin.www.uscc.gov/sites/default/files/Research/10_26_11_CapitalTradeSOEStudy.pdf.

Cyber Methods for Stealing IP

Russia and other states are known to use espionage and cyberattacks on networks to steal defense and other secrets. Hackers stealing trade secrets, money, and personal information are also a worldwide problem. Quantitatively, however, China stands out in regard to attacks for IP. A confluence of factors, from government priorities to an underdeveloped legal system, causes China to be a massive source of cyber-enabled IP theft. Much of this theft stems from the undirected, uncoordinated actions of Chinese citizens and entities who see within a permissive domestic legal environment an opportunity to advance their own commercial interests. With rare penalties for offenders and large profits to be gained, Chinese businesses thrive on stolen technology.

While traditional industrial espionage techniques have been used extensively, cyber methods for stealing IP have become especially pernicious. In a March 2012 report to Congress, the People's Liberation Army (PLA) was identified as a key player, and was noted as often acting in concert with commercial entities. The report suggests that "rather than isolate certain state owned IT firms as exclusively 'defense' in orientation, the PLA…alternately collaborates with China's civilian IT companies and universities." The report concludes that "computer network operations have assumed a strategic significance for the Chinese leadership that moves beyond solely military applications and is being broadly applied to assist with long term strategies for China's national development."[31]

In its study of successful attacks conducted in 2012, Verizon, in cooperation with eighteen private organizations and government agencies, found that "state-affiliated actors" accounted for 19% of the 621 successful "breaches" in the 47,000 attacks reported.[32] Of cases that were deemed motivated by "espionage," the PRC was determined to be responsible for 96%. In spite of the sophistication and reputation of the series of Verizon studies, this figure may exaggerate China's dominance in this arena. Nonetheless, the study adds weight to the findings of the other principal studies in the field, all of which point to China as the major source of state-sponsored attacks on IP.

Similarly, Mandiant Corporation's February 2013 study, entitled "Exposing One of China's Cyber Espionage Units," traces Chinese government sponsorship for cyberattacks on IP. All the industries targeted by the PLA unit studied by Mandiant fall into those considered strategic by the PRC, "including four of the seven strategic emerging industries that China identified in its 12th Five-Year Plan." The PLA unit began operations in 2006, the year that the indigenous innovation policy was approved. The purposes of the cyberattacks were found to be straightforward: to commit espionage and steal data. The unit was judged to access networks over months or even years to "steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organization's leadership." In the words of the report, "the cyber command is fully institutionalized within the CPC [Communist Party of China] and able to draw upon the resources of China's state-owned enterprises to support its operations."[33]

In addition, on May 6 the U.S. Department of Defense issued its 2013 report to Congress on Chinese military developments. Reinforcing the findings from the Mandiant Corporation, the

---

31 Brian Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," prepared for the U.S.-China Economic and Security Review Commission, March 7, 2012, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

32 Verizon RISK Team, "2013 Data Breach Investigations Report," 2013.

33 Mandiant Corporation, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

report notes that the PRC "is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs." It asserts that "the information targeted could potentially be used to benefit China's defense industry, high technology industries, [and] policymaker interest in U.S. leadership thinking on key China issues," among other things.[34]

In a sense, China's current policy toward IP protection is similar to its policy toward environmental protection several years ago. Both IP and environmental protection impose costs and competitive disadvantages on China's highest priority—comprehensive development—and have therefore been widely disregarded. Now, however, Chinese policy is better reflecting the understanding that environmental protection is essential for its citizens to lead healthy lives. Similarly, a solid IPR regime is essential to China obtaining the benefits from innovation necessary to sustain economic progress. Such a regime would encourage Chinese innovation as well as sustain Western innovation, from which China could continue to receive enormous benefits. Although degradation of the atmosphere for innovation is not as obvious as degradation of the air in Chinese cities, the long-term impact is equally devastating.

Problems with Available Trade Mechanisms

Traditionally, in order to solve trade disputes, most developed countries have relied on tools such as unilateral trade sanctions, trade remedies such as countervailing duties, and "voluntary" export restraints.[35] Due to obligations assumed as a result of the World Trade Organization's Uruguay Round negotiations, the United States and other major countries agreed to use WTO mechanisms to settle disputes. The Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), negotiated in 1994 and administered by the WTO, establishes minimum standards for many forms of IP regulation. A qualified success, WTO dispute mechanisms have seen more than 339 settlement reports and arbitration awards issued by the organization's dispute body from 1995 (its year of inception) through 2011. Of these, the United States participated in 140.[36]

Participation rates notwithstanding, WTO dispute mechanisms have several problems. Chief among these is the time required to reach a resolution. The process can be so time-consuming that recapturing any damages through this process is often illusory. As noted above, many products today, especially in the software and other high-tech industries, generate the bulk of profits for their companies in the first weeks or months of release.

Dispute mechanisms for trade in goods have worked reasonably well. However, resolutions to disputes involving IP are often reached behind closed doors, by lawyers lacking a sufficient background to make decisions on important issues of IP protection.[37] This stands in contrast to most modern procedural codes, which generally adhere to common transparent guidelines, including

---

[34] Office of the Secretary of Defense, Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," prepared for Congress, Washington, D.C., 2013, 36, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

[35] Council on Foreign Relations (CFR), "U.S. Trade and Investment Policy," Independent Task Force Report, no. 67, September 19, 2011, http://i.cfr.org/content/publications/attachments/Trade_TFR67.pdf.

[36] World Trade Organization, "Annual Report 2012," 2012, 84–107, http://www.wto.org/english/res_e/booksp_e/anrep_e/anrep12_chap5_e.pdf.

[37] Anne Hiaring, "Fish or Fowl? The Nature of WTO Dispute Resolution under TRIPS," *Annual Survey of International & Comparative Law* 12, no. 1 (2006): 269–288, http://digitalcommons.law.ggu.edu/annlsurvey/vol12/iss1/11.

that "judicial proceedings must be public and that, in principle, the control of the allegations and proof belongs to the parties."[38]

The paucity of legal interpretations of the TRIPS agreement and a general sense of ambiguity inherent in many of the TRIPS obligations have also made it difficult to establish noncompliance and enforce the agreement.[39] For instance, the need for a plaintiff to show clear evidence of systemic failure, as opposed to anecdotal weaknesses in a country's IP enforcement regime, leads to great difficulty in proving a culture of noncompliance under TRIPS for cases in which access to such clear evidence is restricted or otherwise unavailable.[40]

Bilateral and multilateral trade agreements have also often been used to address global IP issues. Such discussions have allowed for more detailed treatment of trade-related issues between the United States and its trading partners that could not be easily dealt with through other avenues, such as the WTO. The Korea-U.S. Free Trade Agreement contains provisions specifically designed to address IP protections. For example, it includes specific provisions for improving enforcement and strengthening the overall legal environment for patents, trademarks, and copyright.[41] The ongoing negotiations of the Trans-Pacific Partnership and U.S.-EU agreements are expected to have similarly high standards for protecting IP. As important as agreements are, however, progress in IP protection often occurs only when U.S. pressure reinforces some preexisting domestic impetus for change.[42]

Recent U.S. Policy Responses Are Inadequate

In addition to participating in WTO dispute mechanisms such as TRIPS, the United States has relied on a series of other measures to deal with IP theft, none of which has solved the problem.

First, the United States has attempted to hector China and other foreign countries into doing a better job of protecting IP. The mechanism utilized annually is the USTR Special 301 Report. As discussed earlier, the report assesses foreign countries on their ability to protect intellectual property and identifies actions taken or anticipated by the U.S. government. In the recently released 2013 report, the USTR notes a grave concern with cyber-enabled trade-secret theft from China. Top administration officials have more frequently decried foreign theft of American IP amid promises to get tough. In March 2013, Thomas Donilon, President Obama's national security advisor, specifically called attention to the problem of Chinese cyber-enabled theft of confidential American proprietary information.[43]

A second U.S. government approach has been to increase enforcement and prosecution initiatives. The Office of the Intellectual Property Enforcement Coordinator was established in 2008 in the Office

---

38 See the discussion in Norbert Horn, Hein Kötz, and Hans G. Leser, *German Private and Commercial Law: An Introduction* (Oxford: Clarendon Press, 1982), 45–50, cited in Hiaring, "Fish or Fowl?"

39 Fanshu Yang, Ping Wang, and Kristie Thomas, "Recent WTO Disputes Involving the Protection and Enforcement of Intellectual Property Rights in China: Legal and Political Analysis," China Policy Institute Briefing Series, no. 24, August 2007, available at http://ssrn.com/abstract=1437642.

40 Ibid.

41 American Chamber of Commerce in Korea, "The KORUS Advantage: A Basic Guide for US Companies to the Contents of the KORUS FTA," November 2012, http://www.uschamber.com/sites/default/files/international/files/KORUS%20Advantage%20Final.pdf.

42 Examples of such agreements have included the U.S.-Japan Structural Impediments Initiative, the U.S.-EU Summit process, and the Security and Prosperity Partnership with Canada and Mexico. See CFR, "U.S. Trade and Investment Policy."

43 See Thomas Donilon, "The United States and the Asia-Pacific in 2013" (remarks presented at the Asia Society, New York, March 11, 2013). Donilon stated: "Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale…. [S]pecifically with respect to the issue of cyber-enabled theft, we seek three things from the Chinese side. First, we need a recognition of the urgency and scope of this problem and the risk it poses—to international trade, to the reputation of Chinese industry and to our overall relations. Second, Beijing should take serious steps to investigate and put a stop to these activities. Finally, we need China to engage with us in a constructive direct dialogue to establish acceptable norms of behavior in cyberspace."

of Management and Budget. Improved legislation and increased enforcement of foreign theft have resulted in the arrest and prosecution of Chinese and other foreign nationals at rates greater than in the past.[44] Seizures by U.S. Customs and Border Protection are also on the rise in many categories.[45]

As important as these efforts are, they just do not have sufficient "teeth" and do not catch perpetrators often enough to make a difference. Theft is increasing, and cyber-enabled forms, in particular, are proving ever more deleterious.

Despite the inadequacy of U.S. government policy and action, many U.S. and other international companies large and small have made the calculation that they can mitigate the risk or absorb the lost revenues and profits. Some U.S. corporate actors are also pursuing their own solutions. Companies such as IBM are supporting the proposed Cyber Intelligence Sharing and Protection Act to allow for greater information sharing between the government and the private sector. Many companies support programs that encourage the rule of law abroad. Others, such as the Center for Responsible Enterprise and Trade (CREATe), seek to standardize best practices for corporate IP policy by enhancing supply-chain accountability on behalf of multinational companies. A final set of actors is increasingly looking to "take matters into its own hands" and pursue unilateral actions, particularly in the cyber domain, against foreign entities that steal their IP.

These conditions cannot be allowed to fester. China has taken aggressive private and public actions that are inflicting major damage to the American economy and national security. Robust and swift action must be taken by the U.S. government. IP thieves must rapidly discover that the costs of stealing American IP greatly exceed the benefits, and several changes are needed to make that happen. This report contains a series of recommendations that will reverse the negative trends of the past and make immediate improvements in the protection of American IP.

Conclusion

While IP theft is not new to the planet, today's scale of economic impacts—with national security ramifications, international dimensions, significant foreign-state involvement, and inadequacy of legal and policy remedies and deterrents—makes for an unprecedented set of circumstances.

China poses an especially difficult problem, given the size and importance of its economy and the interdependence of the Chinese economy with those of the United States, Europe, and Japan. In 1996, Professor Oksenberg and colleagues argued that "Gradually, policy communities supportive and understanding of IPR are arising on the Chinese landscape. In effect, constituencies who stand to gain from IPR are beginning to appear and influence policy. But their strength is relatively weak…"[46] Three and half decades of Chinese economic development and progress in legal reform, together with well-intentioned and improved U.S. policy, have not proved effective. Almost the same things that were said twenty years ago can be restated today, except that now China is the world's second-largest economy and the losses from IP theft have increased greatly. With American companies and workers hurting, millions of jobs, the vibrancy of our innovative economy, and our security are at stake. Meanwhile, the risks for stealing are low and cheating is commonplace.

The starting point for redressing the problem is an understanding of the tools available to fix it. The IP Commission regards access to the American market as the single most important lever

---

[44] See chapter 9 of this report for a thorough description and analysis of recent U.S. government actions to improve the protection of American intellectual property.

[45] See chapter 2 of this report for a discussion of recent seizure rates.

[46] Oksenberg et al., "Advancing Intellectual Property Rights," 29.

in dealing with foreign companies with international ambitions. Thus, the Commission views changing the cost-benefit calculus for foreign entities that steal intellectual property to be its principal policy focus. Stealing American IP needs to have serious consequences, with costs sufficiently high that state and corporate behavior and policies that support IP theft are fundamentally changed. Companies that seek competitive advantages within the American market by using stolen intellectual property must find their access to that market made more difficult or thwarted altogether until they stop stealing.

The forces within China promoting greater IP protection need to be applauded and supported. At the same time, the incentive structure that currently rewards IP theft must be changed. The new Chinese leadership has a great opportunity in this regard. What the Commission can do is recommend specific steps that the United States can take to change the environment of IP theft, while offering to work with all groups in China who see that it is in their interest, as much as ours, to build an effective business environment that protects every country's innovators.

Beyond contributing toward a better functioning Chinese system, the Commission makes a series of recommendations that seek to protect American companies against all sources and forms of IP theft.

Chapter 2

Measuring the Scale and Scope of the Loss of Intellectual Property

After reviewing the extant literature and hearing testimony from a wide range of experts, the IP Commission assesses that when the estimated value of lost sales, stock assets, investments, and other dimensions are added in, the total annual losses due to stolen IP are in the hundreds of billions of dollars.

Technet, a national coalition of CEOs in the high-tech field, estimates that more than six million jobs and more than a third of the United States' $15-trillion economy rely on innovation.[1] A U.S. Patent and Trademark Office study estimates that IP-intensive industries directly accounted for 27.1 million American jobs in 2010, or 18.8% of all employment in the economy. An annual loss of hundreds of billions of dollars of stolen IP—the very lifeblood of America's innovation economy—is indeed extraordinary, especially to a still-recovering U.S. economy.

If the cost is so high and the implications for the U.S. economy so great, why is the IP Commission not able to more precisely measure the loss? The reasons are many.[2] First, loss is necessarily measured in different ways across different sectors and different types of IP theft. For instance, the value of unauthorized software is somewhat easier to measure, in part by counting the number of computers seeking to update software. Similarly, good statistics are kept on the value of seized counterfeit goods entering the United States. On the other hand, some losses are not ever aggregated. Trade-secret losses, for instance, by definition are not included in a total, in part because the value of the loss of an individual company's IP may only become known well after the fact, such as during the trial of a suspected thief or if the company ultimately goes out of business.

A second factor is that companies are highly disincentivized to report their losses for two reasons. First, when a company divulges that it has been a victim of IP theft, there can be certain reputational effects that may affect market confidence in corporate leadership and the value of a company's stock. Second, identifying IP theft almost necessarily requires identifying the source of the theft. If the origin of the theft is in a strategically important market for a company, then a certain level of theft may be written off as merely a "cost of doing business" in an otherwise profitable market.

A third factor centers on the surveys that are often used to measure loss, either by counting the losses reported by survey respondents or by estimating loss from reported statistics. Both approaches are problematic for essentially the same reason. Because IP theft varies widely across sectors and between companies—even within the same sector, companies have widely varying success in protecting their IP—unless every single company is polled and accurately reports its losses, neither aggregating nor estimating has much of a chance of being useful.[3]

What is indisputable is that the scale and scope of the loss is enormous. In a year of research, testimony, and interviews, the IP Commission has not heard one expert suggest the problem is not

[1] See Technet, "America's Innovation Economy," website, http://www.technet.org.

[2] See the Appendix to this chapter for an in-depth report on the challenges of measuring the value of IP theft.

[3] That said, we cite some of these surveys later in the report. Flawed as they might be, they are all that was available. We recognize that we are in some cases drawing conclusions from data that is incomplete.

breathtaking in scale. Even more important than the scale and scope of the loss is an overwhelming assessment by experts that current legal and regulatory approaches to mitigating the loss are staggeringly ineffective.

Below are summaries of a range of highly knowledgeable efforts, which help bound the scale and scope of the problem.

The Details

International Data Corporation (IDC): "The Dangerous World of Counterfeit and Pirated Software" (2013). Counterfeit software is a major vector for the distribution of dangerous malware that imposes substantial costs on the economy and decreases the security of IT systems and data. IDC estimated that globally "the direct costs to enterprises from dealing with malware from counterfeit software will hit $114 billion" in 2013 and "[t]he potential losses from data breaches could reach nearly $350 billion."[4] High rates of IP theft also increase the risks of cybercrime and other security threats, particularly with regard to counterfeit software use.

Bureau of Economic Affairs/U.S. Patent and Trademark Office: "Intellectual Property and the U.S. Economy: Industries in Focus" (2012). The entire U.S. economy relies on some form of IP because virtually every industry either produces or uses it. The report identified 75 industries (from among 313 total) as IP-intensive. These IP-intensive industries directly accounted for 27.1-million American jobs in 2010, or 18.8% of all employment in the economy. The vast majority were in the 60 trademark-intensive industries (which included 22.6 million jobs in 2010).

IP-intensive industries accounted for about $5.06 trillion in value added in 2010, or 34.8% of U.S. GDP. While IP-intensive industries directly supported 27.1-million jobs, either on their payrolls or under employment contracts, these sectors also indirectly supported 12.9 million more supply-chain jobs throughout the economy. In total, 40.0-million jobs, or 27.7% of all jobs, were directly or indirectly attributable to the most IP-intensive industries. Merchandise exports of IP-intensive industries totaled $775 billion in 2010, accounting for 60.7% of total U.S. merchandise exports.[5]

Business Software Alliance: "Shadow Market: 2011 BSA Global Software Piracy Study" (2012). The commercial value of the "shadow market" of globally pirated software climbed from $58.8 billion in 2010 to $63.4 billion in 2011. The study by the Business Software Alliance estimates that the global piracy rate is 42%. The EU rate was judged to be 33%, Japan's is 21%, and the U.S. rate is 19%. However, the piracy rate for emerging economies is over 68%. India's piracy rate is 63% (a 9% decline over the last decade), Russia's rate is 63% (a 24% decline), and Indonesia's rate is 85%.

Meanwhile, China's illegal software market was $9 billion in 2011 out of a total market of nearly $12 billion, for an astonishing piracy rate of 77%. Chinese PC owners spend less than a quarter of the amount of other BRIC countries on software and a mere 7% of U.S. software spending. The BSA study suggests that the problem is only expected to get worse. Emerging markets—the key origins of pirated software—took in 56% of new PC deliveries in 2011.[6]

---

[4] IDC, "The Dangerous World of Counterfeit and Pirated Software," 3–4.

[5] U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," prepared by the Economics and Statistics Administration and U.S. Patent and Trademark Office, March 2012, http://www.esa.doc.gov/sites/default/files/reports/documents/ipandtheuseconomyindustriesinfocus.pdf.

[6] Business Software Alliance (BSA), "Shadow Market: 2011 BSA Global Software Piracy Study," May 2012, http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

U.S. Customs and Border Patrol: Intellectual Property Rights Fiscal Year (FY) 2012 Seizure Statistics. The number of IPR seizures decreased to 22,848 shipments in FY 2012 from 24,792 in FY 2011 (largely due to certain high-volume counterfeited patents leaving service). The estimated manufacturer's suggested retail price for all FY 2012 IPR seizures is $1.26 billion, up from $1.1 billion in FY 2011. China was the source for 72% of seized goods.[7]

International Chamber of Commerce: "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy" (2011). A report commissioned by the International Chamber of Commerce estimates that, based on 2008 data compiled by the Organisation for Economic Co-operation and Development (OECD), the total global economic value of counterfeit and pirated products is as much as $650 billion every year. Moreover, the extent of the problem is expected to grow, in large part as a result of the growth of the Internet. Based on existing estimates, the report also projects that the *global value of counterfeit and pirated products could amount to $1.7 trillion by 2015.* Previous studies have indicated that if counterfeiting and piracy could be eradicated or seriously reduced, up to 2.5-million jobs could be created in the legitimate economies of the G20.[8]

U.S. International Trade Commission (USITC): China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy *(2011).* In 2009, the theft of U.S. IP from China alone was equivalent in value to $48.2 billion in lost sales, royalties, and license fees. This estimate falls within a broad $14.2-billion to $90.5-billion range; the breadth of this range is explained by the fact that many firms were unable to calculate such losses. Of the $48.2 billion in total reported losses, approximately $36.6 billion (75.9%) was attributable to lost sales, while the remaining $11.6 billion was attributable to a combination of lost royalty and license payments as well as other unspecified losses.

The USITC report estimated that an improvement in IPR protection in China to levels comparable to those in the United States could lead to an estimated $107.0-billion gain in U.S. exports and sales to majority-owned affiliates in China (after adjusting for the double-counting of U.S. exports to affiliate firms in China). U.S. exports of goods and services to China—including the receipt of royalties and license fees—could increase by an estimated $21.4 billion, and sales to U.S. majority-owned affiliates in China could increase by an estimated $87.8 billion.[9]

Organisation for Economic Co-operation and Development: The Economic Impact of Counterfeiting and Piracy *(2008).* Quantitative analysis carried out by the OECD indicates that the volume of tangible counterfeit and pirated products in international trade could have been up to $200 billion in 2005.[10] This figure does not, however, include counterfeit and pirated products that are produced and consumed domestically, nor does it include the significant volume of pirated digital products that are being distributed via the Internet. If these items were added, the total magnitude of counterfeiting and piracy worldwide could well be several hundred billion dollars more. The OECD report also finds that 70% of the source economies of IP theft are in the Asia-Pacific region.

---

[7] Office of the Intellectual Property Enforcement Coordinator, "Intellectual Property Spotlight," January/February 2013.

[8] International Chamber of Commerce, "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy," February 2011, http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study.

[9] USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, 3-37, http://www.usitc.gov/publications/332/pub4226.pdf.

[10] *The Economic Impact of Counterfeiting and Piracy* (Paris: OECD, 2008).

Effects on R&D and Innovation

Regardless of how overall monetary value of IP loss is quantified, the true losses extend far beyond decreased revenues and lost market share. There are also secondary effects that directly influence companies to significantly reduce their R&D investments, thus slowing long-term economic progress. Reduced incentive to innovate, diversion of revenues to IP-infringing firms and away from IP-creating firms, and diversion of revenues to IP-protection measures and away from R&D investment are just a few of the reasons that companies may struggle to maintain investment in innovative activity.

Reduced Incentive to Innovate

IP protections in the United States are based on the fundamental belief that providing limited monopolies to inventors and creators incentivizes further innovation, driving forward human and economic development.[11] A 2011 study conducted for the U.S. Chamber of Commerce's Global Intellectual Property Center examined the contributions of IP-intensive industries in the U.S. economy and concluded that they were responsible for up to a third of U.S. economic output.[12] This economic growth, however, is not limited to specific industries or classes; the benefits of IP are felt across all sectors and, to some extent, affect every job in the economy. As explained in a recent report by the U.S. Patent and Trademark Office, "every job in some way produces, supplies, consumes, or relies on innovation, creativity, and commercial distinctiveness. Protecting our ideas and IP promotes innovative, open, and competitive markets."[13]

While the argument that strong IP protections are an overall benefit to the economy has historically been a theoretical and anecdotal one, it has garnered an increasing body of empirical support.[14] Recent studies have shown that the level of a country's IP protections is a key determinant of its overall economic development.[15] In an OECD study of WTO TRIPS (trade-related aspects of intellectual property rights) signatories, researchers found that patent rights in developing countries tended to be positively associated with increased levels of FDI as the strength of those rights increased.[16] It is important to note, however, that IP protections are only beneficial to an economy when they are adequately enforced.[17] The lack of enforcement is the key issue in many countries. As one expert noted when discussing Chinese IP rights, "the problem is not the lack of laws…. The problem is implementation."[18]

---

11 U.S. Const. art. I, § 8; and Andréanne Léger "Intellectual Property Rights and Innovation in Developing Countries: Evidence from Panel Data" (paper prepared for presentation at the International Association of Agricultural Economists Conference, Gold Coast, Australia, August 12–18, 2006), 2, available at http://bit.ly/15oAEA9.

12 Nan D. Pham, "Employment and Gross Output of Intellectual Property Companies in the United States," NDP Consulting, January 2011, 4, available at http://bit.ly/JvExFv.

13 "Intellectual Property and the U.S. Economy: Industries in Focus," Economics and Statistics Administration, U.S. Patent and Trademark Office, March 2012.

14 "Measuring Momentum: GIPC International IP Index," Global Intellectual Property Center Index, U.S. Chamber of Commerce, December 2012, 9, available at http://bit.ly/ZCLQlz.

15 Theo S. Eicher and Monique Newiak, "Intellectual Property Rights as Development Determinants," *Canadian Journal of Economics* 46, no. 1 (2013).

16 TRIPS refers to "trade-related aspects of intellectual property rights." See W.G. Park and D. Lippoldt, "The Impact of Trade-Related Intellectual Property Rights on Trade and Foreign Direct Investment in Developing Countries," Organisation for Economic Co-operation and Development (OECD), May 21, 2003, 4, available at http://bit.ly/11p7cF0.

17 Park and Lippoldt, "The Impact of Trade-Related Intellectual Property Rights," 4.

18 Adam Segal, *Advantage: How American Innovation Can Overcome the Asian Challenge* (New York: W.W. Norton, 2012).

When IP protections are strong and effective, they can provide tremendous incentive for innovators, create jobs, and drive broad economic development, especially in sectors where returns on investment are long term.[19] Conversely, when IP is not protected, the incentive structure for individuals and firms changes, with start-up companies being the clear losers.

Revenues Diverted to IP Infringers

When a country fails to provide adequate protection for intellectual property, the result is not only a lost incentive to innovate but also a positive incentive to infringe. In all the IP-intensive industries there exist both IP creators and IP infringers. The former use their time, money, and human resources in the pursuit of new and better inventions and vary in size from large multinational corporations to small start-ups operating out of a garage. What they all have in common is a drive to create, with the expectation that the market will reward them for their ingenuity. IP infringers do not create. They instead use the creative powers of other firms or individuals to generate revenue for themselves. Examples include industrial spies stealing proprietary chemical formulas, patrons of cybercriminals who break into corporate networks in order to steal trade secrets for use in their own products, DVD and software pirates across Asia, and manufacturers of counterfeit luxury goods. When these infringers are allowed to succeed in their endeavors, we allow the marketplace to reward and incentivize IP theft. This state of affairs creates a vicious cycle, whereby ill-gotten revenues are utilized to continue to fund the firm's standing business model of IP theft.

Clearly, while both IP infringers and creators can generate revenue from an economy, only one of these business models creates lasting, long-term economic growth.

Revenues Diverted to IP Protections

Most firms see R&D expenditures as investments in their long-term growth. As outside firms and individuals steal IP, firms increasingly spend revenue trying to protect their previous R&D investments from being stolen rather than on new R&D investments.[20] Rampant infringement of IP in China has been directly cited by U.S. firms as a reason for reduced expenditures on R&D, and even reduced employment in the U.S.[21] Why would these companies continue to spend from a continually shrinking pot on new R&D investments when they cannot protect the return on their previous investments?

According to the previously cited USITC report, "firms in the U.S. IP-intensive economy…spent approximately $4.8 billion in 2009 to address possible Chinese IPR infringement."[22] Again, the hardest-hit sector was information services. Furthermore, a company's costs for protecting its IP on the Internet are increasing rapidly. A recent study estimated that the median annualized cost to organizations of cybercrime for 50 benchmarked companies was $5.9 million per year and ranged

---

19 "The Impact of Intellectual Property Protection on Innovation and Technology Development," Business and Industry Advisory Committee to the OECD, January 2003, available at: http://bit.ly/XVDH0m.

20 U.S. Government Accountability Office (USGAO), "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit or Pirated Goods," Report to Congressional Committees, GAO-10-423, April 2010, 12.

21 USITC, *China: Effects of Intellectual Property Infringement*, 2-7, 2-21.

22 Ibid.

from $1.5 million to $36.5 million per company.[23] Smaller companies have suffered the most and incur almost four times the per capita cost of large companies.[24]

Beyond lost incentives and fewer resources, a lack of IP protection also incentivizes unfair competition. Not all stolen IP comes in the form of a final product. In many cases, stolen IP is used as an input to make what would otherwise be classified as legitimate goods. For instance, a fishing company in Thailand was recently fined for using pirated software to manage its business infrastructure.[25] By using illegal software, this company was able to operate at significantly lower cost than its IP-respecting counterparts, resulting in an unfair advantage. When these violations are allowed to persist, business practices become a race to the bottom. Forced to compete on a tilted playing field, other companies will also begin to use stolen IP simply to remain competitive in the marketplace.

Regardless of the specific reason, it is clear that the theft of IP is proving to be an inhibiting factor in realizing the value of currently held IP while depriving firms of funding aimed at the production of new IP. In the face of staggering losses, firms will have less motivation to innovate, have less money to invest in R&D, and hire fewer employees. They will also continue to be distracted by attempts to chase down the perpetrators of IP theft in a desperate, and often futile, attempt to stem their losses.

The studies give sobering evidence that the United States, along with other countries, faces one of the greatest and most vexing political-economic challenges in history. America's core economic strength is being attacked successfully on a mammoth scale, and we are well into the game.

---

[23] Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies," Research Report, August 2011, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[24] Ibid.

[25] "Company Fined for Using Pirated Software to Gain Unfair Advantage over Massachusetts Businesses," Attorney General of Massachusetts, Press Release, October 18, 2012.

Appendix: Challenges in Measuring IP Loss

Studies often begin with disparate views as to what should be counted when measuring IP theft, resulting in wide variation between studies in terms of the bottom-line value of IP theft. In general terms, these definitions of "what counts" include:

- *Effects on industry.* Lost sales; lost brand value; reduced scope of operations; lost jobs and reduced ability to provide employee benefits; reduced ability to conduct R&D; increased IP protection expenses for prevention, remediation, and enforcement; increased costs from dealing with malware acquired from unlicensed software; reduced incentive to innovate.
- *Effects on government.* Lost tax revenue; increased IP protection expenses for prevention, remediation, and enforcement, including costs to store, secure, and destroy seized assets; benefit to criminal networks looking to launder money or harm the public; impact on national security; impact on civilian safety, in that illegally obtained goods and processes that depend on IP might not have safety-dependent updates (in the case of software) or appropriate protections may have been left out or deleted (in the case of counterfeit goods).
- *Effects on consumers.* Harm to health, harm to safety, costs incurred as a result of product failure, decreased or increased purchasing power.
- *Effects on the U.S. economy as a whole.* Decline in economic growth as incentives to innovate are reduced, lost trade revenue, impact on the environment; increase in companies with substandard working conditions.

Most existing research on IP theft uses one or more of the following indicators to create a broad yet sizeable estimate:

- *Volume of goods (VOG) seized by U.S. Customs and Border Protection (CBP).* While often used as a baseline for estimates, the limitations of using VOG include uncertainty regarding whether it reflects the aggregate of the loss, whether the assessed percentage of loss can be known, or simply whether it represents the maximum volume that CBP is able to capture given its resources. CBP seizures are an inadequate metric for a number of categories of loss, including digital piracy and trade-secret theft.
- *Dollar value of goods seized by CBP.* In using the value of seized goods in estimating total loss, one must first determine whether to measure production cost, domestic value, the manufacturer's suggested retail price, or some interim price point depending upon methodology.[26] As with VOG, it is also unclear if these numbers reflect the totality or a set fraction of the problem, or simply the maximum volume that CBP is able to capture given its resources. It is also a poor measure of digital piracy.
- *Ratio of the volume or value of illegitimate goods to legitimate goods in a particular industry.* This approach often uses CBP data as a primary indicator, but can use specialty formulas derived from surveys.
- *Extrapolations based upon consumer surveys.* This methodology often attempts to combine quantitative data (how many goods were pirated) with more qualitative data (how much value was actually lost based upon knowledge of consumer behavior).

  Survey questions may focus on the following: customer willingness to pay for counterfeit goods; personal ethics regarding piracy; number of illegitimate purchases during a set timeframe;

[26] For example, BSA and IDC use a formula that suggests that the value of pirated goods = [(legitimate market value) / (1- piracy rate) – legitimate market value]. However, this formula does not appear to be universal.

minimum expectations regarding quality; pricing points that would eliminate incentives for piracy; awareness of and reactions to penalties or side effects (including health, safety, and legal).

This method can be especially useful for measuring losses in software or other digital products that are not reflected in CBP data. Surveys can ask consumers to indicate how many of a certain unit they have installed to estimate total products available and then subtract that number from the known number of units sold. Negative numbers can indicate the extent of piracy in a given industry.

However, a survey approach has limitations. It can be cost and labor intensive, it can be distorted by reporting bias, and is subject to the quality of the survey design.

- *Economic multipliers.* This approach shows how capital changes in one industry affect output and employment in associated industries.

  The Bureau of Economic Analysis at the Department of Commerce has published guidelines that make regional multipliers available through its Regional Input-Output Modeling System (RIMS II).

- *"Rule of thumb."* The U.S. Government Accountability Office (USGAO) argues that there is no reliable "rule of thumb" for estimating the percentage of a given industry that is dominated by piracy.

Other difficulties to bear in mind in the measurement challenge include the following:

- Many agencies such as the Department of Commerce and the FBI rely on industry statistics rather than original research, which can result in inconsistent or unverifiable methodologies.
- Some industries do not want to expose the scale of counterfeiting and thus may underreport. Increased IP theft may increase overall revenue directed towards a particular IP, as sampling results in greater product exposure. IP theft can allow companies to "move into the aftermarket"—effectively acquiring knowledge that can allow them to become true competitors rather than solely continuing to copy products. This phenomenon may be even more difficult to capture in a cost assessment.
- Research by the USGAO indicates that three widely cited studies on the impact of counterfeiting on the U.S. economy—attributed to the FBI, CBP, and FTC—"cannot be substantiated due to the absence of underlying studies," creating additional challenges for researchers.

Chapter 3

Types of IP Theft

IP theft varies widely in both type and method. It ranges from more commonly known forms, such as software and music piracy, to more elaborate types, such as the use of economic espionage tactics to steal complex industrial trade secrets. Each type of IPR violation harms an economy in unique ways and brings with it a discrete set of challenges that make both deterrence and enforcement difficult.

In the chapters that follow, we discuss each type of IP theft, how it is perpetrated, how it affects the local economy, how it costs American jobs, and why each type is so inherently difficult to stop. The anecdotes we use are real, documented stories, based on facts largely available in the public domain. They support some of our early conclusions as a commission—namely, that IP theft in general is substantially human, manifestly local, and unceasingly pervasive.

The stories that most people hear or imagine when thinking about IP theft, economic espionage, or trade-secret theft are the grist of high-tech espionage thrillers. However, while it is true that the rise of personal computing has added a new dynamic to protecting intellectual property, it is important to remember that nearly all IP loss, no matter how high-tech, still requires a human component. It is rare that a significant violation is perpetrated through cyber methods alone. In order for IP theft to be successful, a human element is needed. While cyber methods add new challenges, the fight is still human.

Additionally, the mention of global IP thieves often conjures up images of a foreign enemy based somewhere on the other side of a vast ocean. State-sponsored efforts immediately leap to mind—for example, Shanghai-based PLA Unit 61398, which has been identified as the source of many recent cyberattacks.[1] In reality, however, most IP theft is committed within American offices, factories, and even neighborhoods and homes. Our research has shown that large IP losses, the ones that affect the American economy and national security in the most significant ways, are committed within U.S. borders.

Finally, IP theft and its effects are not isolated to a few high-tech industries or sectors. There are a total of 27-million jobs within the U.S. IP-intensive economy, which is nearly 20% of all jobs in the American economy.[2] However, IP is used everywhere and in nearly all jobs. Even though a sector may not be dedicated to creating IP, it still uses intellectual property or is in some way supported by industries that are within the IP-intensive economy. With an economy as interconnected as ours, when IP is lost in one sector, the negative effects of this loss are felt throughout.

In the chapters that follow, we examine the global environment with regard to IP theft through case studies and analysis in the areas of patent, trade-secret, trademark, and copyright law.

---

[1] "Chinese Cyber-attacks: Hello, Unit 61398," *Economist*, February 19, 2013, http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks.

[2] U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," prepared by the Economics and Statistics Administration and U.S. Patent and Trademark Office, March 2012.

Chapter 4

Patent Violations

Viewing China's development of a patent system in a global historical context provides a vivid illustration of the large amount of progress that the country has achieved in a relatively short period of time. Patent protection, along with copyright, was one of the earliest forms of IP protection, formally dating to fifteenth-century Italy and the Venetian Statute of 1474. In England, the late Tudors (c. 1561) initiated the practice of issuing "letters patent" granting monopolies on the manufacture and sale of commodities. The policy was intended to attract foreign craftsmen and tradespeople to settle in the country and make use of their knowledge and skills domestically.[1] This practice was extended by Elizabeth I and later James I into the early seventeenth century to encompass the inventions of native Englishmen as well, solidifying the granting of monopolies as a discretionary means of extracting income and maintaining political power.[2]

By the end of the reign of James I, changes began to occur that would alter the political and social landscape, eventually giving birth to a diverse intellectual environment tolerant of opposing viewpoints. A fairly developed patent system emerged, along with institutions to enforce an individual's claim to original creation.[3] The process began with the deprecation of the royal issuance of letters patent for monopolies by Parliament in 1621.[4] This was immediately followed by the promulgation of the Statute of Monopolies in 1624, the first patent law formally defining invention, and setting a fourteen-year period as the standard for patents.[5] The statute also stipulated parliamentary approval for all patents, although a compromise in section 6 allowed the crown to retain power of letters patent only when issued to "the true and first inventor" of "new manufactures." This would remain the effective patent law for all of England's industrial revolution until 1852, when a new law established a patent office.[6]

In the United States, patent rights were authorized in Article I of the Constitution: "The Congress shall have power.… To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."[7] The United States has generally maintained this utilitarian view by providing patent protection with the belief that it would incentivize innovation and economic development. Thomas Jefferson, one of the first patent commissioners, wrote in a 1789 letter to James Madison that the Bill of Rights should include the language "monopolies may be allowed to persons for…their own inventions in the arts for a term not exceeding—years but for no longer term and no other purpose."[8] The founders believed that this

---

1 Ron Harris, "Government and the Economy, 1688–1850," in *The Cambridge Economic History of Modern Britain Volume 1: Industrialisation 1700–1860*, ed. Roderick Floud and Paul Johnson (Cambridge: Cambridge University Press, 2004), 204–37; and UK Intellectual Property Office, "Tudors and Stuarts," http://www.ipo.gov.uk/types/patent/p-about/p-whatis/p-history/p-history-tudor.htm.

2 UK Intellectual Property Office, "Tudors and Stuarts."

3 See Lyman Ray Patterson, *Copyright in Historical Perspective* (Nashville: Vanderbilt University Press, 1968); and Douglass C. North and Robert Paul Thomas, *The Rise of the Western World: A New Economic History* (Cambridge: Cambridge University Press, 1973).

4 Nigel Stirk, "Intellectual Property and the Role of Manufacturers: Definitions from the Late Eighteenth Century," *Journal of Historical Geography* 27, no. 4 (2001): 475–92.

5 Ibid.

6 Harris, "Government and the Economy, 1688–1850."

7 U.S. Const. art. I, § 8, cl. 8.

8 Thomas Jefferson to James Madison, "On The Liberty to Write, Speak, and Publish and Its Limits," August 28, 1789.

inherently "monopolistic" policy generally incentivized innovation. If researchers and inventors are not assured a reasonable expectation of return, they are less likely to expend time, money, and energy in developing new innovations. This is especially true in today's modern economy, where R&D expenditures for new high-tech innovation can run into the billions of dollars. When patent laws are violated or inventions misappropriated internationally, incentive for innovation is greatly reduced and revenue is diverted from innovating companies to infringing companies. A review of the 2012 Special 301 report from the office of the USTR indicates that although there has been progress rooting out patent violations, infringing activities and weak patent regimes remain a global problem even in some of the world's largest economies.

China itself has made great progress in its nascent patent system. In the fewer than three decades since the introduction of a modern patent regime in China (enacted in 1985), the PRC has become the leading country in the world in terms of the number of patents filed in domestic offices. Over the past decade and a half alone, domestic patent applications have increased from around 105,000 in 1997 to over 1.6 million in 2011.[9] This flurry of activity may be seen as a response to a concerted government effort to spark innovative activity. It is led not only by many of the largest Chinese companies (e.g., the technology companies ZTE and Huawei) but also by many smaller companies taking advantage of government incentives such as tax breaks and financial rewards available to firms that actively file patents both domestically and abroad.[10] Yet while the overall numbers may create an impression of increased innovative activity, they should be taken with caution. The evidence suggests that the steep increase in the number of patents reflects in part a greater incentive simply to patent, rather than to innovate. This "ecosystem of incentive" provides tenure to professors, *hukou* (residence) permits to students and workers, cash bonuses and rebates to filers, and even bonuses to patent examiners based on the number of patents approved.[11]

Patent Infringement[12]

A study by the U.S. International Trade Commission found that U.S. firms estimate losses to Chinese patent infringers to have topped $1.3 billion in 2009 alone.[13] Although many of these companies could not identify whether or not they thought patent infringement had either increased or decreased during the polling period of 2007–9, substantially more thought that it had increased (24%) than decreased (<1%).[14] A significant number of these companies also noted that as a result of

---

[9] Figures cover both resident and nonresident applications. See World Intellectual Property Organization (WIPO), Country Statistical Profiles (China), http://www.wipo.int/ipstats/en/statistics/country_profile/countries/cn.html.

[10] WIPO, Country Statistical Profiles (China). See also "China to Provide Financial Incentives for Filing Patent Applications Abroad," China IPR, web log, June 12, 2012, http://chinaipr.com/2012/06/12/china-to-provide-financial-incentives-for-filing-patent-applications-abroad.

[11] "Innovation in China: Patents, Yes; Ideas, Maybe," *Economist*, October 14, 2010, http://www.economist.com/node/17257940.

[12] Infringement of a patent occurs when a non-patent holder practices all the steps of the patented invention without authorization, whether or not that entity was previously aware of the existence of the patent. Infringement can be direct or indirect. In both the United States and China, direct infringement requires one actor to perform each step of the patented method or system. U.S. law allows for two types of indirect infringement, contributory and induced. 35 U.S.C. § 271(b) defines induced infringement as "[w]hoever actively induces infringement of a patent shall be liable as an infringer" and requires the patentee to show that another person actually infringed and that the alleged inducer knew of the patent and, nevertheless, knowingly induced the infringing acts with a specific intent to encourage infringement by that person. Contributory infringement requires that there is direct infringement, that the accused infringer had knowledge of the patent, that the component has no substantial non-infringing uses, and that the component is a material part of the invention. China does not have specific doctrine related to indirect infringement; rather, claims for all forms of IPR infringement are handled under its Tort Liability Law, under which section 8 provides for joint and several liability for tortious acts in general. See Patrick E. King, Timothy T. Lau, and Gautam V. Kene, "Navigating the Shoals of Joint Infringement, Indirect Infringement, and Territoriality Doctrines: A Comparative Analysis of Chinese and American Patent Laws," *Columbia Journal of Asian Law* 25, no. 2 (2012): 275, 277, 81. *See also Vita-Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1328 (Fed. Cir. 2009); and *Fujitsu Ltd. v. NETGEAR Inc.*, 620 F.3d 1321, 1326 (Fed. Cir. 2010).

[13] USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, 3-37, http://www.usitc.gov/publications/332/pub4226.pdf.

[14] Ibid., 3-40.

the losses, they put less money into R&D and were forced to divert funds to legal costs that otherwise would have gone to R&D.[15]

Industries with high levels of R&D expenditures, such as biotechnology, high-technology, and pharmaceutical companies, typically rely on the protection provided by patent systems (usually for twenty years or more) to recoup expenses in product development and realize profit from their inventions. In this way, patents provide incentive to these companies to continually innovate. Patents not only form the core of the assets for large R&D-centric companies but also offer important protection for the inventions of small start-up companies that may be seeking early-round venture capital investment.[16]

The Utility Model Patents

One result of the recent Chinese emphasis on the volume of patents has been an exponential increase in the number of utility model patents. Utility model patents, sometimes referred to as "petty patents," are distinct from invention model patents in that they confer a patent term of ten years instead of twenty, require only a basic description of the subject matter being patented, and do not require an extensive examination in order to determine whether the subject matter of the application is actually innovative.[17] Although China is not the only country with a patent law that allows such patents—several other countries, including Germany, Japan, South Korea, and Australia, feature utility model patents as part of their system—no other country makes such extensive use of this form. While these patents were originally intended to spur innovation by serving as a limited-time protection and are restricted in their use to physical goods, the speed with which they can be obtained and their effectiveness as a tool in litigation have resulted in a dramatic upsurge in this type of patent.[18] Filing of utility model patents in China was already on the rise in the mid-2000s, but it began to explode at the start of China's indigenous-innovation campaign in 2006 and after Schneider Electric, a French electronics company, lost a landmark $45-million case in 2007. The case was brought by Chint Group, a Chinese company that held a utility model patent for a miniature circuit breaker similar to one sold by Schneider.[19] Between 2007 and 2011, filings by residents for utility model patents, which had been growing at an increasing rate of about 10,000 to 20,000 per year for nearly a decade, ballooned from 180,000 to 580,000 per year. By way of contrast, the second-largest filer of utility model patents, Germany, saw only about 16,000 total utility model applications in 2011.[20]

An unfortunate side effect of the state-led indigenous-innovation campaign, as well as the rush to file patents following high-value verdicts, is that patents granted under China's utility model system are creating a "patent thicket." U.S. companies must now navigate through a large volume of patents that may be of questionable value if they desire to operate in China.[21] A recent report prepared by Thomas Moga for the U.S. Chamber of Commerce concluded that utility model patents in China not only do not serve their original purpose of encouraging inventors. Because they are cheap, not

---

15 USITC, *China: Effects of Intellectual Property Infringement*, 3-40.

16 Ibid., 3-37.

17 Ibid., 3-40.

18 Bob Stembridge, "Chinese Utility Models—A Lesser-Known IP Strategy," *Intellectual Asset Management Magazine*, July/August 2010.

19 "France's Schneider Loses China Patent Case—Xinhua," Reuters, September 29, 2007.

20 WIPO, Country Statistical Profiles (China).

21 Thomas T. Moga, "China's Utility Model Patent System: Innovation or Deterrent?" U.S. Chamber of Commerce, November 2012, http://uscham.com/V5aXyq.

rigorously examined, quickly granted, and difficult to invalidate, these patents have in fact become "disruptive to normal business growth" and may even be leading to a rise in nonpracticing entities (i.e., patent trolls) that seek to register patents that may already exist abroad for the sole purpose of litigating against these foreign patent holders if they seek to enter the Chinese market.[22] Utility model patents based on questionable research, copied ideas (sometimes even including photocopies of old patents in the applications), and even old, invalidated technology are being pursued and granted in record numbers.[23]

These are not the only reasons, however, for the proliferation of low-quality patents in China. A 2012 report by the European Chamber of Commerce in China also noted that the problem is systemic, stating that it is rooted "in a wide range of policies and other measures, as well as administrative and enforcement approaches, that do not seem to be effectively addressed at present, nor on course to be effectively addressed, and in some cases are not even discussed at all."[24]

The rise of utility model patents has produced a multitude of negative consequences in China for U.S. companies. One consequence is higher business transaction costs as a result of uncertainty with regard to the scope and validity of granted patents, whether an invention is patentable, or whether a patent will even be enforced. Another negative effect is the encouragement of unnecessary patent disputes, resulting in greater litigation costs. In addition, this system has created an increasing cycle of patent abuse whereby domestic parties in China race to file utility model patents based on recently disclosed foreign patents or leaked product images or descriptions. They then sue the foreign company when it tries to market these products in China.[25] According to a Beijing-based attorney at the international law firm Orrick, Herrington & Sutcliffe, one can "literally copy patents from any country and have them filed and granted in China as a utility model patent."[26] It appears that Chinese companies are using such means to stockpile utility model patents with the goal of going after foreign companies as soon as they seek to enter the Chinese market.[27] Dan Prud'homme, manager of the IPR and R&D groups at the European Chamber of Commerce in China, remarked to an IP-management publication that some sources put the number of utility model patents filed with the intent of being asserted offensively at 50%. He further argued that there are many "concerning cases" where patents were "filed on inventions that were already part of the prior art and were used as harassment tools, barriers to entry and restrictions on freedom to operate."[28] This trend makes it increasingly evident that the utility model system is being abused to provide what is effectively a state-sanctioned tool for the extortion of global businesses.

Anecdotally, such extortion appears to be becoming increasingly flagrant. In a recent instance of harassment in fall 2012, Hong Kong company Goophone released a product purportedly based on a leaked image of Apple's iPhone 5 and promptly threatened to sue Apple if it proceeded to release its

---

22 Moga, "China's Utility Model Patent System," 8.

23 Ibid., 15–16, citing Toby Mak, *CIPA Journal* (April 2011): 235. Mak pointed to utility model patent ZL200520124981.7, which was a literal copy of the earlier granted utility model patent ZL02270703.4.

24 Dan Prud'homme, "Dulling the Cutting Edge: How Patent Related Policies and Practices Hamper Innovation in China," European Chamber of Commerce, August 2012, 18.

25 Ibid., 40.

26 Julian Evans Pritchard and Annie Mark, "Innovate, Litigate, or Tax Rebate?" Caixin Online, September 11, 2012, http://english.caixin.com/2012-09-11/100436101.html.

27 Jane Denny, "New Litigation Dangers Emerge in China," *Intellectual Asset Management Magazine*, October 25, 2011, http://www.iam-magazine.com/blog/detail.aspx?g=7d14a2b9-34ca-495c-9d8d-ec18d892cbae&q.

28 Joff Wild, "Chinese Authorities Plan to Take Action on Bad Faith Utility Model and Design Patent Applications," *Intellectual Asset Management Magazine*, February 22, 2013.

as-yet-unannounced smartphone in China.[29] Among other things, Goophone threatened to assert its patents for the design of the phone—a claim that indicates Goophone's use of the utility model patent framework to obtain fast coverage of the leaked design.[30] To be sure, Chinese authorities recognize that there are substantial problems with this system as it is applied in China and are taking steps to address these issues.[31] Recent publications from the U.S. Chamber of Commerce and the EU Chamber of Commerce in China have made several recommendations aimed at bolstering the utility model system in China.[32] Among these suggestions are recognizing the statutory requirement for innovation in utility model patents, meaning an actual evaluation of inventiveness; adopting the requirement that the loser pays court costs in lawsuits; making utility model patents easier to invalidate by broadening the scope of what is admissible as prior art; reducing barriers to obtaining preliminary injunctions; and strengthening rules on discovery and evidence preservation. All of these measures would provide strong disincentives to abuse the utility model system in China.

[29] Dexter Roberts, "Enter Goophone I5, Looking a Lot Like Apple's iPhone 5," *Bloomberg Businessweek*, September 6, 2012, http://www.businessweek.com/articles/2012-09-06/enter-goophone-i5-looking-a-lot-like-apples-iphone-5.

[30] Joff Wild, "Apple's Chinese iPhone 5 Patent Problem Is Probably Not a Problem at All," *Intellectual Asset Management Magazine*, September 9, 2012.

[31] Prud'homme, "Dulling the Cutting Edge," 26, 29–33.

[32] See, for example, Prud'homme, "Dulling the Cutting Edge"; and Moga, "China's Utility Model Patent System."

Chapter 5

Trade-Secret Theft

Patents only represent one method for protecting the competitiveness of inventions in the marketplace. Due to public-disclosure requirements for patent protection and the difficulty of enforcing patents in other nations and markets, many firms choose to keep their competitive edge by opting not to patent their inventions and trying instead to keep them as trade secrets.[1] A famous example of this calculus dates to late eighteenth-century England, where overly ambiguous patents led to almost a century of stalled innovation with regard to the development of the steam engine.[2] This state of affairs would influence famed porcelain manufacturer Josiah Wedgewood to abandon the patent process entirely, resorting instead to constant innovation and secrecy in order to maintain his lead in the porcelain industry.[3]

Protecting proprietary information as a trade secret, however, poses its own challenges and may not be any safer than the patent process. Foreign firms and individuals are increasingly focusing on the theft of trade secrets, primarily through two avenues: industrial and economic espionage and cyber espionage.

Industrial and Economic Espionage

Titanium dioxide, also known as titanium white, is one of the most valuable and ubiquitous chemicals in the world. It has been used to whiten consumer goods such as car paint, sunscreen, paper, plastics, toothpaste, and cosmetics, and was even used to paint the Saturn V rocket. If a product is white, it probably contains titanium white. In 2012, it was estimated that the worldwide market value for the pigment was $17 billion, with DuPont controlling nearly 20% of that market.[4]

As manufacturing has increased exponentially in China and other Asian countries, the demand for titanium white has also increased. After DuPont refused to sell its proprietary manufacturing process to China, the Chinese began looking for different avenues to obtain DuPont's secret chlorination production method. According to an indictment filed by the FBI, the "People's Republic of China (PRC) publicly identified the development of chloride-route titanium dioxide (TiO2) production technology as a scientific and economic priority."[5] Prosecutors believe that in the 1990s, Walter Liew, a California resident, assembled a team of former DuPont employees for the purposes of conveying the company's proprietary technology to entities in the PRC.[6] Pangang Group Co. Ltd., a Chinese state-owned enterprise, awarded Liew a $17 million contract to build a factory in China that could produce 100,000 metric tons of titanium white.[7] The FBI listed five individuals within the United

---

1 "Intellectual Property: Can You Keep a Secret?" *Economist*, March 16, 2013, http://www.economist.com/news/business/21573580-patent-idea-you-must-publish-it-many-firms-prefer-secrecy-can-you-keep-secret.

2 Nigel Stirk, "Intellectual Property and the Role of Manufacturers: Definitions from the Late Eighteenth Century," *Journal of Historical Geography* 27, no. 4 (2001): 475–92.

3 Ibid., 479.

4 Paul Elias, "Economic Spying Case over DuPont's Chemical Grows," Associated Press, March 10, 2012, available at http://finance.yahoo.com/news/economic-spying-case-over-duponts-160258759.html.

5 *United States v. Pangang Group International Economic & Trading Company*, 2012 WL 400340 (N.D. Cal.).

6 *United States v. Walter Lian-Heen Liew*, 2012 WL 400340 (N.D. Cal.).

7 Elias, "Economic Spying Case."

States and a number of Chinese entities and individuals as defendants in conspiring to steal the formula from DuPont. One of the U.S. defendants, Tze Chao, who worked at DuPont from 1966 to 2002, was charged with conspiracy to commit economic espionage.[8] Pangang officials allegedly hired Chao and instructed him to work with Liew in Liew's "development" of the DuPont formula.[9] In his guilty plea, Chao told prosecutors that officials from the PRC "overtly appealed to my Chinese ethnicity and asked me to work for the good of the PRC."[10]

While federal prosecutors successfully obtained a plea bargain from Chao, their case against Pangang Group has been less successful. In an attempt to bring Pangang officials to court, on February 9, 2012, the U.S. government delivered a summons for each of the Pangang Group defendants to Brenda Kong. Ms. Kong was the office manager at a company called Pan America, which is owned in part by Pangang Group.[11] The trial judge, however, held that serving the court summons to Pan America was an improper method for serving Pangang Group and quashed the indictment. Pangang now runs the largest titanium complex in China and is one of the country's largest titanium white producers.[12]

Industrial espionage is nothing new. It is a classic business tactic used by less than reputable organizations to try and obtain a competitor's secrets in order to gain an economic advantage in the marketplace. The USITC reported that in 2009 U.S. firms in the IP-intensive economy lost roughly $1.1 billion from the misappropriation of trade secrets to China alone.[13] The range of this estimate is particularly uncertain because many victims of economic espionage and trade-secret theft are unaware that they were ever robbed.[14] Among those who are aware of their losses, many choose to not report them for business reasons.[15] While many U.S. firms are noting some improvement in other areas of IPR protection, protecting trade secrets remains a significant challenge internationally, particularly in China.[16] Industrial espionage, however, is not only a problem in China. The Office of the National Counterintelligence Executive, after noting China as a "persistent collector," stated that Russia,

> motivated by [its] high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward U.S. and other Western interests at the expense of Russia, [is] using [human intelligence], cyber, and other operations to collect economic information and technology to support Russia's economic development and security.[17]

---

8 Elias, "Economic Spying Case."

9 *Liew*, 2012 WL 400340 (N.D. Cal.).

10 "FBI Traces Trail of Spy Ring to China," *Wall Street Journal*, March 10, 2012.

11 *United States v. Pangang Group Co., Ltd.*, 879 F. Supp. 2d 1052, 1056 (N.D. Cal. 2012).

12 Karen Gullo, "Former DuPont Worker Pleads Guilty in Economic Espionage Case," Bloomberg, March 2, 2012, http://www.bloomberg.com/news/2012-03-02/former-dupont-worker-pleads-guilty-in-trade-secrets-case.html.

13 USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, 3-37, http://www.usitc.gov/publications/332/pub4226.pdf.

14 Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011, October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

15 Ibid.

16 USTR, "2012 Special 301 Report," April 2012.

17 Office of the National Counterintelligence Executive, "Foreign Spies."

The report maintained that both China and Russia would "remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace."[18]

In many ways, trade-secret theft is a foreseeable outgrowth of expanding international markets. When large multinational companies expand their overseas operations, they almost inevitably face challenges related to supply accountability and protection against such theft. Their foreign manufacturing operations and joint-venture partners require customer lists, internal standards, manufacturing processes, information on sources of goods, recipes, and production and sales strategies in order to carry out their operational responsibilities.[19] Each new piece of information that is sent oversees opens a company's supply chain and puts its valuable IP at risk.

Another reason that trade-secret theft and economic espionage are so challenging to curtail is because it is notoriously difficult to enforce current law within the established legal framework. In the mid-1990s, the U.S. Congress responded to the growing problem of international trade-secret theft by passing the Economic Espionage Act of 1996 (EEA). When President Clinton signed the legislation, he stated that the new law "will help us crack down on acts like software piracy and copyright infringement that cost American businesses billions of dollars in lost revenues. And it will advance our national security."[20]

The EEA criminalized two distinct actions: economic espionage and theft of trade secrets. Economic espionage is defined as stealing, misappropriating, or receiving trade secrets while "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."[21] Theft of trade secrets, on the other hand, is defined as stealing, misappropriating, or receiving such secrets "with intent to convert [the] trade secret… to the economic benefit of anyone other than the owner thereof."[22]

Thus, the key distinction between economic espionage and theft of trade secrets is who benefits. Economic espionage is done for the benefit of a foreign nation, whereas theft of trade secrets is done for the economic benefit of an individual or organization.

Because economic espionage requires that the act be done with intent to benefit a foreign nation, it is a much more difficult crime to prosecute. The first conviction for economic espionage under the EEA was handed down in *United States v. Dongfan Chung* in 2009. Chung, who is a Chinese native and U.S. citizen, was a stress engineer at Boeing who worked on the fuselage for the U.S. space shuttle, among other projects.[23] Upon arresting him, federal prosecutors found 300,000 pages of documents in his home, including "a veritable treasure trove of Boeing's documents relating to the Space Shuttle, Delta IV Rocket, F-15 fighter, B-52 bomber, CH-46/47 Chinook helicopter, and other proprietary aerospace and military technologies."[24] Chung was convicted of economic espionage and sentenced to fifteen years in prison.

It is more common, however, for federal prosecutors to charge a defendant with trade-secret theft because it does not require that they prove the defendant acted with intent to benefit a foreign power. One example is the case of Xiang Dong "Mike" Yu, who pleaded guilty in 2010 to trade-secret theft

---

18 Office of the National Counterintelligence Executive, "Foreign Spies."

19 Center for Responsible Enterprise And Trade (CREATe), "Trade Secret Theft, Managing the Growing Theft in Supply Chains," 2012.

20 Bill Clinton, "Statement on Signing the Economic Espionage Act of 1996," October 11, 1996, available from Government Printing Office, http://www.gpo.gov/fdsys/pkg/WCPD-1996-10-14/html/WCPD-1996-10-14-Pg2040.htm.

21 *Economic Espionage Act of 1996*, Public Law 104-294, codified at U.S. Code 18 (1996), §1831.

22 Ibid., § 1832.

23 Ann Woolner et al., "The Great Brain Robbery," *Bloomberg Businessweek*, March 15, 2012.

24 *United States v. Dongfan Chung*, 633 F. Supp. 2d 1135 (C.D. Cal. 2009).

after copying 4,000 proprietary documents right before leaving his job at Ford. He then took the documents with him to his new job at Beijing Automotive. Yu was sentenced to nearly six years.[25]

One important aspect of the EEA is its extraterritorial jurisdiction component. The law protects against theft in three instances: the act occurred in the United States; the act occurred outside the United States, but an act in furtherance of the offense was committed in the United States; or the violator is a U.S. person or organization.[26] Thus, the EEA can be used both to prosecute foreign persons and to prosecute theft outside the United States as long as either the violator is a U.S. person or organization or an act in furtherance of the offense was committed in the United States.[27] While this semi-broad reach is useful in defining trade-secret theft, it is still limited in that prosecutors lack enforcement and proper service mechanisms against individuals and entities located outside the United States, such as Pangang Group. Prosecutors cannot charge alleged violators of the EEA until they cross U.S. borders.

In a recent development, on December 28, 2012, President Obama signed the Theft of Trade Secrets Clarification Act. The act was a response to a recent case involving a Goldman Sachs programmer who, on his last day at work, transferred 500,000 lines of source code to a private server to take with him to his new job.[28] After the trial court found him guilty of theft of a trade secret, the Court of Appeals for the Second Circuit overturned this conviction, holding that the stolen code was not a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce."[29] The new law rewords § 1832(a) of the EEA by removing this limitation on its application and instead broadening the statute to apply to "a product or service used in or intended for use" in interstate or foreign commerce.[30] This minor change expands the EEA's reach in two ways. First, it removes the limitation of trade secrets to goods (which the U.S. Court of Appeals for the Second Circuit recently held does not include software code) and defines services as secrets as well.[31] Second, it removes the limitation on the law's applicability to goods to be placed in interstate or foreign commerce, expanding it to goods or services to be used or intended for use in interstate or foreign commerce.

This expanded reach may give the United States an added tool to prosecute IP-infringement activities abroad. Nonetheless, while this clarification helps strengthen the definition of crimes under the EEA, its extraterritorial reach remains limited. Once a secret has been stolen and the perpetrator has left the country, there is little a prosecutor can do to enforce the law. Furthermore, there is nothing a victim of economic espionage can do because the EEA currently does not provide for a private civil cause of action for victims. The limits of the EEA are especially conspicuous when looking at the number of cases prosecuted under the law. Since the passage of the EEA in 1996, there have been only around one hundred indictments and a handful of convictions.[32] Notably, of the seven cases adjudicated under the EEA in 2010, six involved some link to China.[33]

---

25 Woolner et al., "The Great Brain Robbery."

26 FBI, "Economic Espionage," http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.

27 Ibid.

28 *U.S. v. Sergey Aleynikov*, 676 F.3d 71, 73 (2nd Cir. 2012).

29 Ibid.

30 *Theft of Trade Secrets Clarification Act of 2012*, S. 3642, available at http://thehill.com/images/stories/blogs/flooraction/jan2012/s3642.pdf. The act rewords language in § 1832(a) of the EEA.

31 *Aleynikov*, 676 F.3d 71, 76.

32 "Intellectual Property: Can You Keep a Secret?"

33 Office of the National Counterintelligence Executive, "Foreign Spies."

Cyberespionage

The rise of the Internet has provided the world the fastest and most effective communications system in history. However, this system, in conjunction with traditional espionage methods, is being used to steal some of U.S. businesses' most valuable trade secrets. In the past two years, an unprecedented number of cyberattacks have been uncovered against major corporations, nonprofit institutions, and governments alike. The vast majority of these attacks have been traced back to China. A single attack against RSA, the maker of the widely used SecurID tokens, resulted in the compromise of at least 3 major defense contractors.[34] The same attack compromised security at an estimated 720 companies, including 20% of the Fortune 100.[35] Through another series of attacks, dubbed operation Shady RAT, it was discovered that petabytes of highly proprietary information, including sensitive military and infrastructure data, had been siphoned off from the U.S. government and its allies, supranational organizations such as the United Nations, and many other sovereign nations and independent organizations over a period of more than five years.[36] Notably, General Keith Alexander, the head of the U.S. military's Cyber Command, said that one U.S. company alone recently lost $1 billion worth of intellectual property over the course of a couple of days.[37]

In a world where the highest-value assets are intangible and easy to transfer over networks, espionage has taken on a new dimension. The size and scale of recent attacks point to state sponsors, meaning that such events are no longer being perpetrated by ad hoc groups operating in the shadows but are much more organized and nationalized. According to a report released on November 1, 2011, representing fourteen U.S. intelligence agencies, such attacks will accelerate in coming years as a "growing and persistent threat."[38] In its white paper on Shady RAT, McAfee indicated that the attack was more than likely the work of a group operating on behalf of a state actor. While not calling out China specifically, the geographical data discovered by McAfee's cyber forensic team on the spread of the attack strongly suggests China's involvement.[39]

These attacks are having a devastating effect on U.S. economic interests both at home and abroad. Throughout 2011 and into 2012, the cost to organizations of cybercrime continued upward unabated. A 2011 study by the Ponemon Institute found that the median annualized cost for 50 benchmarked companies was $5.9 million per year and ranged from $1.5 million to $36.5 million per company. This is a $2.1 million, or 56%, increase from the median cost of $3.8 million to benchmarked companies in 2010. The study also found that smaller organizations incur almost four times the per capita cost ($1,088) as larger organizations ($284) in dealing with cyberattacks.[40]

In addition, the Ponemon study found that cyberattacks are common occurrences, with participating companies experiencing 72 successful attacks per week—an average of 1.4 per

---

34 Zeljka Zorj, "RSA Admits SecurID Tokens Have Been Compromised," Help Net Security, June 7, 2011, http://www.net-security.org/secworld.php?id=11122.

35 Brian Krebs, "Who Else Was Hit by the RSA Attackers?" Krebs on Security, web log, October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers.

36 Peter Bright, "Operation Shady Rat: Five-Year Attack Hit 14 Countries," Ars Technica, August 3, 2011, http://arstechnica.com/security/news/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries.ars; and "Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China," Fox News, August 3, 2011, available at http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china.

37 Ellen Nakashima, "In a World of Cybertheft, U.S. Names China, Russia as Main Culprits," *Washington Post*, November 3, 2011.

38 Siobhan Gorman, "China Singled Out for Cyber Spying," *Wall Street Journal*, November 4, 2011.

39 Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee, August 2011.

40 Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies," Research Report, August 2011, http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf.

organization polled—representing a 44% increase from the previous year.[41] This figure is consistent with recently available information from Cisco Systems, which found a 46% increase in web malware during the first quarter of 2011 alone, with malicious webmail increasing by an astounding 391%.[42] The Ponemon study also found that the major costs from these intrusions were those related to information theft (40%), followed closely by costs associated with disruption to business and lost productivity (28%).[43]

Web- and email-based malware attacks continue to gain prominence as a prime attack vector for cybercriminals. Most such attacks operate by sending a targeted person or group of people a personalized email and convincing them to open an attachment containing malicious software that grants the cyberattacker broad access to their systems. The malware is thus intended to be executed by the target on the same day (or close to the same day) that it is sent. Such "zero day" attacks are highly customized and take advantage of previously unknown software vulnerabilities that prevent detection by existing antivirus or signature-based systems installed at most organizations. During the fourth quarter of 2011, 33% of web malware encountered by Cisco Systems was zero-day in nature and not detectable by the traditional signature-based systems at the time of attack.[44] The onslaught of zero-day attack vectors is reflected in the increase in web malware hosts, as recorded by Cisco, from an average 14,217 per month in 2010 to 20,141 in 2011—a 30% increase.[45] Likewise, in an April 2012 report, Symantec recorded an increase in the number of advanced persistent threats from an average of 77 per day in 2010 to 82 per day in 2011.[46] The Symantec report noted that such attacks differ from conventional targeted attacks in key ways, including by employing a high degree of customization, using stealthy and patient methods to avoid detection, being more tightly focused on gaining access to high-value information and organizations of strategic importance, and displaying signs of originating from well-funded and highly staffed operators (such as military or state intelligence organizations).[47]

Of further concern, it is now clear that companies and industries in every sector are being targeted, although the extent to which they are suffering attacks varies by industry segment. The Ponemon study's findings indicate that the three top sectors being targeted are defense, utilities and energy, and financial services, although even companies in retail, hospitality, and consumer products are under fire.[48] This data largely tracks with the "Cisco 4Q11 Global Threat Report." Pharmaceutical and chemical companies topped the list of companies targeted with malware at 422% of the median, followed closely by agriculture and mining and energy, oil, and gas.[49] Finally, Symantec's 2011 report also makes the important point that it is not just large companies that are being hit by targeted attacks. To the contrary, more than half of all targeted attacks recorded by Symantec in 2011 were directed at companies with fewer than 2,500 employees and almost 18% targeted companies with 250 or fewer employees. Adding to the difficulty in preparing for and intercepting such attacks, the

---

41 Ponemon Institute, "Second Annual Cost of Cyber Crime."

42 Cisco Systems, "Cisco 1Q11 Global Threat Report," 2011, http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_global_threat_report_1Q2011.pdf.

43 Ibid.

44 Cisco Systems, "Cisco 4Q11 Global Threat Report," 2012, http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_4Q11.pdf .

45 Ibid.

46 Symantec, "2011 Internet Security Threat Report," April 2012, 14, available at http://www.symantec.com/threatreport.

47 Ibid., 15.

48 Ponemon Institute, "Second Annual Cost of Cyber Crime," 4.

49 Cisco Systems, "Cisco 4Q11 Global Threat Report," 4.

majority tend to target lower-level employees, who may lack direct access to sensitive information but be more susceptible to compromise.[50]

In the rapidly evolving landscape of cyberespionage, it has become clear that not even the smallest organizations or lowest-level employees are safe from attack. Of equal concern is that effective and deeply penetrating cyberattacks are occurring across a broad spectrum of IP-intensive industries. Unfortunately, despite pressing China on the issue for several years, none of the United States' diplomatic efforts seem to have had any effect in abating the scale of the threat. Then U.S. defense secretary Leon Panetta remarked after a recent trip to China that the most important thing was that China was willing to even engage in a dialogue on the issue of cyberattacks.[51] Richard Bejtlich, president of the cybersecurity firm Mandiant, described the issue more bluntly, stating that the efforts of U.S. and Chinese officials have lacked any impact at all and that "the Chinese don't seem to care. So I don't have any hope that the dialogue is reaching anyone of note."[52]

[50] Symantec, "2011 Internet Security Threat Report," 17.

[51] Lolita C. Baldor, "Chinese Cyber Attacks on U.S. Continue Totally Unabated, Leon Panetta Complains," Associated Press, September 20, 2012.

[52] Baldor, "Chinese Cyber Attacks."

Chapter 6

Trademark Violations

Apple is one of the most popular brands in the world, so when an Apple store was opened in the city of Kunming, China, its six million residents were excited to take advantage of the products and services offered. The new store came complete with the large distinct wooden tables, sleek interior design, large colorful advertisements, and helpful staff members wearing the blue shirts donned by Apple store employees worldwide.[1] Everything was seemingly in place, except for one major problem—this was not actually an Apple store. The store in Kunming had appropriated Apple's trademarks and trade dress—even convincing its own employees that they were working for Apple itself—in order to sell Apple products and provide Apple-branded services, all without the company's permission.[2]

Some have argued that the public's initial shock at the discovery of these fake stores was overblown. The products being sold by the store appear to have been legitimate Apple products, even though the source of the products was unknown.[3] The example, however, clearly demonstrates the ubiquity of trademark infringement internationally and the lengths to which infringers are willing to go in order to convincingly counterfeit goods and services, diverting profits from trademark owners to themselves.

A "trademark" is simply a word, phrase, symbol, or design that identifies and distinguishes the sources of the goods of one party from those of others.[4] Unlike the protections granted to patents and copyrights, trademark protection is not directly derived from the U.S. Constitution. For many years, it only existed as a common law right derived from a party's actual usage of the mark and defended in state courts.[5] It was not until Congress passed the first federal trademark law in 1881, under its Commerce Clause authority, that trademarks received nationwide protection.[6] Since that time, trademark jurisprudence has grown substantially. Statutes have been continually amended and updated under the Lanham Act, originally enacted as a federal trademark statute in 1946 and frequently amended since that time.[7]

Unlike patents and copyrights, trademarks do not confer protection for the use or replication of specific products. Trademark protection can be violated in several ways. For one, trademarks can be infringed when they are misappropriated. Misappropriation occurs when an existing mark is replicated onto a product without the trademark holder's authorization (counterfeiting).[8] The most ubiquitous examples are purses or shoes available at sidewalk stands in cities such as New York and

---

1 Minning Yu, "Benefit of the Doubt: Obstacles to Discovery in Claims against Chinese Counterfeiters," *Fordham Law Review* (April 2013).

2 Melanie Lee, "Fake Apple Store Even Fools Staff," Reuters, July 21, 2011.

3 "Mitt Romney Called Out on Fake Apple Store," *Wall Street Journal*, China Realtime Report, October 17, 2012, http://blogs.wsj.com/chinarealtime/2012/10/17/china-fake-apple-store-blogger-romney-misusing-the-story.

4 U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," prepared by the Economics and Statistics Administration and U.S. Patent and Trademark Office, March 2012.

5 "Overview of Trademark Law," Harvard University, Berkman Center for Internet and Society, http://cyber.law.harvard.edu/metaschool/fisher/domain/tm.htm

6 Ibid.

7 *Lanham Trademark Act of 1946*, Public Law 79–489, codified at U.S. Code 15, § 1051, available at http://www.law.cornell.edu/uscode/text/15/1051.

8 Andrew C. Mertha, *The Politics of Piracy: Intellectual Property in Contemporary China* (Ithaca: Cornell University Press, 2005).

Beijing (and increasingly on auction websites) that are not authorized by the owner of the brand they carry. In addition, trademarks can be infringed on when a manufacturer uses marks or design elements very similar to those of a competitor in order to confuse consumers and trick them into purchasing a product.[9] Strong trademark protections provide significant benefits to an economy by allowing entities to derive benefits from investment in their brands. Where trademark protection is weak, both consumers and producers suffer. Consumers are hurt because they may be receiving an inferior product or service, while producers suffer because they will reap a lower reward for their investment in their mark. Perhaps worse, if the trademark is famous, producers may suffer from brand dilution or other negative effects on their brand's reputation as a result of the infringement.

Consumers benefit from trademark protection in a number of ways, all stemming from the information trademarks provide about a product's origin and quality. This in turn, creates a positive incentive for companies to create higher-quality, longer-lasting products. When a company uses its trademark on goods or services that it provides, it will generally work to ensure that the goods are of a sufficiently high quality to maintain its identity in the marketplace. In this way, strong trademark protections allow brands to serve as a signal of quality to the consumer. Simply put, such protections foster the development of better goods and services.[10]

Producers, for their part, benefit from strong trademark protection because it helps them maintain long-standing relationships with consumers. For instance, when a company produces high-quality products, provides excellent service, and invests in carefully marketing its products, it builds goodwill that translates into a higher level of consumer confidence. Consumers will express this confidence by returning to the company repeatedly, generating long-term revenue streams for the producer. When these elements are not present, however, consumers may be dissuaded from purchasing future products or services from that company.

The Economic Costs of Counterfeiting

Counterfeiting is a rampant practice in countries that possess even a modest manufacturing industry. The list of consumer goods that are counterfeited is long and includes apparel, footwear, mobile phones, herbal remedies, computer and networking equipment, batteries, cigarettes, cosmetics, home appliances, cement, auto parts, and more. The bulk of losses to American business in the light and consumer-goods manufacturing sector is primarily due to trademark violations and counterfeit products.[11] When a consumer purchases a counterfeit good, the true trademark holder loses that revenue.

Some observers have argued that estimates of losses are exaggerated because of potentially low substitution rates. The argument is that a consumer who purchases lower-priced counterfeit goods would not have purchased a legitimate product if the fakes were not available. Therefore, the true trademark holders have not actually lost revenue. While this may be true for some small physical markets, many of these counterfeit products are frequently showing up for sale on eBay, Amazon Marketplace, Craigslist, and other legitimate websites with access to a global consumer base, where unsuspecting customers may believe that they have found a discounted legitimate product rather

---

9 Mertha, *The Politics of Piracy*.

10 Ibid.

11 USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, 3-37, http://www.usitc.gov/publications/332/pub4226.pdf.

than a fake.[12] If consumers believe that they are buying a legitimate product to begin with, chances are that they still would have purchased one if the knock-off were unavailable.

Furthermore, the loss to producers is much more significant than the immediate loss of revenue. There is also a long-term threat to the brand itself. Whether it is cosmetics, appliances, apparel, or auto parts, counterfeit goods frequently fall short of the industry and quality standards by which legitimate goods are measured. As they enter the marketplace, low-quality knock-off goods and services can hurt a company's reputation by decreasing consumer confidence, diluting the brand, and harming long-term revenues. Revisiting the Apple example, the fake Kunming store offered repair and support services for the Apple products it sold. However, because the employees had not been trained according to Apple's standards, the quality of service they offered is unknown. To the extent that the technical support and customer service provided at these illicit outlets were below the exceptionally high standard set by Apple in its own stores, such experiences could damage Apple's reputation in the eyes of customers, leading them to purchase products from another source in the future.

Overall, rampant trademark infringement lowers product quality, decreases consumer confidence, and reduces legitimate business revenue.

Barriers to Enforcement and Recovery

In a 2009 USITC survey of U.S. companies, more firms reported losses from trademark infringement by Chinese entities—an estimated $6.1 billion in losses in that year alone—than from other forms of Chinese IPR infringement. When these losses could be attributed to a specific market, 37.7% identified China, 32.3% identified the United States, and 30.1% identified "all other markets."[13] This spread illustrates that the problem is not just trademark infringement inside China but also involves goods being shipped into the United States. In fact, U.S. Customs and Border Protection announced that it made "22,848 intellectual property rights seizures with a manufacturer's suggested retail value of $1.26 billion" in 2012, with goods from China responsible for 72% of this amount.[14] Companies have also reported problems registering their trademarks in China, including long backlogs that require a wait of up to two years, trademarks with similar names being registered by competitors, companies registering an identical mark in a different product class, and "squatting" by people who register someone else's trademark as their own.[15] The latter is a problem specific to China's system, which grants rights to the first person to file for a trademark, whereas the U.S system protects the party who is first to use the mark in commerce. Even as companies gain traction on policing their own brands in China, counterfeiting continues to grow. Factors include the shift from traditional centers such as Guangzhou to smaller "living room" operations, continued lax penalties for retailers selling fake goods, and the growth of Internet sales, such as on eBay, Taobao, or Alibaba.[16] Online sales of counterfeit goods, in particular, have been growing at an alarming rate. U.S. Customs and Border Protection reported a shift in 2007–11 toward lower-value shipments

---

12 USITC, *China: Effects of Intellectual Property Infringement*, 3-37.

13 Ibid., 3-31.

14 Counterfeit handbags and wallets constituted roughly 40% of seizures in 2012, followed by watches and jewelry (15%), and apparel and accessories (11%). See "Intellectual Property Rights Fiscal Year 2012 Seizure Statistics," U.S. Customs and Border Protection, 2012, http://1.usa.gov/13WftmP.

15 USITC, *China: Effects of Intellectual Property Infringement*, 3-34.

16 Ibid., 3-33.

by international mail and express courier, presumably to individual buyers, and away from larger container shipments to bulk purchasers.[17]

In a series of recent decisions, courts in China have also indicated a change from their earlier reasoning that using trademarks on goods while manufacturing items for export constitutes "use" of the mark.[18] This would allow, for example, Nike to enforce its Chinese trademark rights against the manufacturer producing shoes for sale in Spain, where another entity holds the rights to the Nike mark. Through these decisions, it appears that Chinese courts are increasingly willing to consider such original equipment manufacturing activities to be a form of "reasonable use," and that it should also be required to show that such use is likely to result in confusion among consumers in the relevant Chinese market as to the source of the goods.[19] These decisions could make it more difficult for brand owners to enforce their trademarks in China by closing one door they had previously used to shut down the manufacture of goods bearing their mark. These decisions also leave unanswered the question of how Chinese courts will determine the legitimate owner of the mark in the destination country, as well as how they will determine the "relevant public" in evaluating the likelihood of confusion.[20]

Given the large number of companies reporting trademark-related losses attributable to Chinese IPR violations that occur in the United States, and the high value of items being seized by U.S. Customs and Border Protection, owners of global brands have begun to fight back through the U.S. legal system. Notably, Gucci America and Tiffany have been attempting to obtain information on parties in China who have been selling counterfeit goods over eBay.[21] A recent report described the problems that these companies encountered in trying to obtain bank and contact information regarding the absentee defendants. Established protocols under the Hague Convention have proved both slow-moving and unfruitful, with Chinese banks frequently citing secrecy laws as a shield against discovery of the counterfeiters' bank account information.[22] Without access to this information, it is impossible for the companies that are suffering losses due to trademark infringement to calculate the value of their losses and uncover other potential defendants in cases where sellers were acting as middlemen for the original manufacturer.[23]

These examples make clear that U.S. companies face a sobering local environment for protecting their trademarks within China. Companies continue to have difficulty tracking down perpetrators utilizing global websites, payment systems, and the international mail system. The next chapter examines the subject of copyright and presents the staggering rate at which this form of intellectual property is being exploited and stolen.

---

17 "Intellectual Property Rights Fiscal Year 2011 Seizure Statistics," U.S. Customs and Border Protection, 2011.

18 George Chan, August Zhang, and Chris Bailey, "OEM and the Concept of 'Reasonable Use' of a Trademark," *World Trademark Review*, April/May 2013, 72.

19 Ibid.

20 Ibid., 75.

21 *Gucci America, Inc. v. Weixing Li*, no. 10 Civ. 4974(RJS), 2011 WL 6156936 (S.D.N.Y. August 23, 2011); Tiffany (NJ) LLC v. Qi, No. 10 Civ. 9471(WHP) (S.D.N.Y. January 3, 2011); and *Tiffany (NJ) LLC v. Forbse*, no. 11 Civ. 4976(NRB) (S.D.N.Y. August 3, 2011).

22 Yu, "Benefit of the Doubt," 3001-02.

23 Ibid., 3008.

Chapter 7

Copyright Infringement

In 1999, a political scientist was in an economically well-developed area of China studying, ironically, intellectual property rights. While interviewing an official who worked in the Office of the Education, Science, Culture, and Public Health Committee of the Provincial People's Congress, the researcher mentioned that he was interested in purchasing a CD-ROM set of China's national and local laws, but even at the reduced price of $1,000, this was more than the academic could afford. The government official took the researcher to a market notorious for openly selling pirated software. The researcher walked away with the entire set for roughly $1.50.[1]

Copyright law protects original works of authorship that are in a fixed, tangible form of expression.[2] Put another way, copyright protects the expression of ideas.[3] Like patent protection, copyright was one of the early forms of IP protection afforded by the U.S. Constitution.[4] While such protection originally covered tangible items like books and paintings, over time Congress and the courts have extended it to include audio recordings, movies, and computer software.[5] A common form of copyright infringement is the production of pirated goods, which are any goods made without the consent of the copyright holder. These may take the form of physical books or DVDs in a market in Shenzhen or digital downloads made available to a broader audience via the Internet.[6] The purpose of copyright protection, again similar to patent protection, is to maintain a positive incentive to write, create, and publish new works, since such innovation is generally seen as an overall benefit to society.[7]

The USITC estimates that copyright infringement is the most costly form of IP loss for the United States with respect to China, costing U.S. producers nearly $24 billion in 2009.[8] Not surprisingly, IP theft has hurt the information services industry the most, with losses in 2009 of nearly $26 billion.[9] Globally, some estimates place the commercial value of software theft at over $60 billion.[10] Yet the true cost remains unknown for numerous and sometimes contradictory reasons. First among these is the unknown substitution rate.[11] Many studies simply calculate how many versions of a particular piece of software are currently installed on computers and compare it with how many copies were sold.[12] They then multiply that figure by the retail price to determine "lost revenues," or the value

---

1 This story is told at length and in greater detail in Andrew C. Mertha, *The Politics of Piracy: Intellectual Property in Contemporary China* (Ithaca: Cornell University Press, 2005).

2 U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," prepared by the Economics and Statistics Administration and U.S. Patent and Trademark Office, March 2012.

3 Mertha, *The Politics of Piracy*.

4 U.S. Const. art. I, § 8.

5 Mertha, *The Politics of Piracy*.

6 USGAO, "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit or Pirated Goods," Report to Congressional Committees, GAO-10-423, April 2010.

7 Mertha, *The Politics of Piracy*.

8 USITC, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, no. 332-519, USITC Publication 4226, May 2011, http://www.usitc.gov/publications/332/pub4226.pdf.

9 Ibid.

10 BSA, "Shadow Market: 2011 BSA Global Software Piracy Study," 9th ed., May 2012.

11 USGAO, "Intellectual Property."

12 See, for example, BSA, "Shadow Market."

lost if all software installations had been purchased legally. The problem with this approach is that if piracy were not an option, some of these consumers, particularly in low-income economies, would never purchase the software because it is priced too high.[13]

On the other hand, studies that use survey methods to estimate losses may provide estimates that are too low because many companies opt to not report their losses for financial and business reasons.[14] As an example, one high-tech software company that the Commission spoke to in its investigation reported that it had sold a single copy of a piece of software to a bank in China. Later, 30 million copies of software traced to that single license contacted the corporate servers of this company for software updates. Between this anecdote and countless others, it is clear that the true loss to companies from piracy is difficult to accurately measure but unarguably substantial.

China is not alone in its high piracy rates; software piracy is in fact a global problem. In 2011, many countries exceeded China's piracy rate of 77%, including Vietnam (81%), Pakistan (86%), and Venezuela (88%).[15] Yet though the higher piracy rates in these and other countries should not be ignored, the sheer size of the Chinese market makes it the most significant focus for improvement. In 2011, China had the second-largest commercial value of pirated software at nearly $9 billion. Russia was third with $3.2 billion, while first place belonged to the United States, with a commercial value of pirated software approaching $10 billion. However, with a piracy rate of only 19%, the United States had nearly $39 billion more in legitimate sales.[16]

Ukraine was recently declared to be a "priority foreign country" by the U.S. Trade Representative in its annual Special 301 Report—the first country given this designation in seven years.[17] The report cites Ukraine's persistent failure to combat online piracy as a primary reason for its 301 status. Most striking, however, is the pervasive use of illegal and unlicensed software within the Ukrainian government itself. Industry reports show similar findings. According to a study by the Business Software Alliance, the country's piracy rate has hovered around 85% since 2007 and has shown no improvement.[18] In contrast, Ukraine is not listed by the BSA as one of the top-twenty possessors of pirated software as measured by commercial value. Presumably, this is due to the relatively small size of the Ukrainian software market.[19]

While pirated software is the most highly publicized form of international and domestic copyright infringement, the entertainment industry also experiences significant losses from piracy. A 2007 study estimates that the U.S. economy loses $12.5 billion in total output annually due to piracy of sound recordings.[20] A similar 2007 study estimates that movie piracy now results in total lost output among all U.S. industries of $20.5 billion annually.[21] As with similar software piracy studies, however, these estimates are limited by uncertain substitution rates.[22] In China, 99% of all music downloads are illegal. The total music revenue in the country for 2010, including both digital and physical sales,

---

13 USGAO, "Intellectual Property."

14 Ibid.

15 BSA, "Shadow Market."

16 Ibid.

17 USTR, "2013 Special 301 Report," May 2013.

18 BSA, "Shadow Market."

19 Ibid.

20 Stephen E. Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," Institute for Policy Innovation, Policy Report, no. 188, August 2007.

21 Ibid.

22 USGAO, "Intellectual Property."

was only $64 million. To put this figure in perspective, it is less than total sales in Thailand, which registered $68 million in sales in 2010.[23] Thailand has a population and GDP (based on purchasing power parity) twenty times smaller than that of China. If China had purchased the same amount of music on a per capita basis as Thailand, a country not known for staunch IP protections, sales would have been nearly $1.4 billion.[24]

[23] USTR, "2013 Special 301 Report."

[24] International Monetary Fund, World Economic Outlook Database, April 2013.

Chapter 8

U.S. Government Responses

U.S. administration efforts to date have made important strides in protecting intellectual property, although much work remains to be done. The position of the Intellectual Property Enforcement Coordinator (IPEC) was established by Congress through the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act). The administration housed the position within the Office of Management and Budget, staffing it with members of various bureaucracies, largely from the enforcement side. Veteran U.S. trade negotiator and IP counsel Victoria Espinel was appointed the first IPEC. The administration has pushed forward on the following five policy fronts.

1. Joint Strategic Plan on Intellectual Property Enforcement

The administration released the Joint Strategic Plan on Intellectual Property Enforcement in June 2010. The plan's central tenets included 33 action items to improve intellectual property enforcement, falling into six categories:[1]

1. Leading by example and working to ensure that the U.S. government does not purchase or use infringing products
2. Being transparent in policymaking and enforcement
3. Improving coordination of law enforcement at the federal, state, and local levels; of overseas personnel; and of international training efforts
4. Enforcing U.S. rights internationally in order to ensure that the United States is effectively working with foreign governments
5. Working to secure the U.S. supply chain by attempting to limit the infringing products entering the country
6. Building a data-driven government and ensuring that U.S. policies are as well-informed as possible by improving data collection on IP-enforcement efforts, measuring the economic impact of IP industries, and assessing U.S. laws to ensure that they effectively protect and enforce IP rights

2. Foreign Economic Espionage Penalty Enhancement Act

The Foreign Economic Espionage Penalty Enhancement Act of 2012 (H.R. 6029) was signed into law by President Obama on January 14, 2013. This act significantly increases maximum penalties for the misappropriation of trade secrets to benefit a foreign government, allowing penalties of up to $5 million for individuals and up to three times the actual value of the trade secret for organizations. This is a significant increase from the respective $500,000 and $10 million caps on penalties that limited the effectiveness of the previous version of the statute. Because the new law is equipped to more adequately reflect the actual value of a stolen trade secret, it may provide greater incentive for prosecutors to pursue EEA violations, while increasing pressure on violators of U.S. trade-secret laws.

[1] The following list draws from the Executive Office of the President of the United States, "Joint Strategic Plan on Intellectual Property Enforcement," 2010.

The passage of this bill came shortly after the Theft of Trade Secrets Clarification Act of 2012, which was signed into law on December 28, 2012, and expands section 1832 of the EEA to include trade secrets "related to a product or service used in or intended for use in interstate or foreign commerce." Taken together, these two modifications to the EEA provide important new enforcement and deterrent tools to prosecutors.

Despite their usefulness, more still needs to be done. There is currently no federal private right of action under the EEA for those who hold trade secrets. Thus, only government prosecutors can file lawsuits in order to seek redress for violations of the statute. Such a bill was introduced in July of last year (the Protecting American Trade Secrets and Innovation Act of 2012, S. 3389), but the Senate Judiciary Committee chose to not act on the bill. The recent speedy passage of the Foreign Economic Espionage Penalty Enhancement Act and the Theft of Trade Secrets Clarification Act, however, indicates a shift in momentum favoring legislation designed to protect U.S. intellectual property. Both bills were rapidly passed with nearly unanimous votes and were quickly signed into law by the president.

3. Executive Order on Cybersecurity

The administration has also recently issued an executive order on cybersecurity that:

- directs increased sharing of unclassified information from government entities to private-sector providers of critical infrastructure;
- proposes to bring more subject-matter experts from the private sector into temporary government service;
- increases the quantity and specificity of threat information to the private sector;
- establishes a consultative process to coordinate improvements to the cybersecurity of critical infrastructure;
- directs the National Institute of Standards and Technology to develop a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework); and
- develops procedures for implementing a risk-based approach to determining which infrastructure is most vital.[2]

While this executive order is an important first step, there are some challenges. First, although the potential impacts of the budget sequester are still unclear, it could conceivably result in fewer resources being available to accomplish these tasks, especially in view of their urgent timelines. Second, while the goal of increased information-sharing is important and laudable, the executive order does not create new authorities for such sharing. It essentially tells government agencies to do a better job than they are doing now. Third, the order does not protect the sharing of information from a request or lawsuit under the Freedom of Information Act, nor can it. Only Congress can create these important protections. Fourth, the direction to the National Institute of Standards and Technology to develop guidelines, which other agencies are then directed to implement, is a compliance-oriented approach that may not actually increase security. As technology and the nature of the threats constantly evolve, regulations will have a hard time keeping up.

[2] "Executive Order—Improving Critical Infrastructure Cybersecurity," White House, Executive Order, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Perhaps most importantly, the executive order does not address what can or ought to be done against perpetrators. With such an approach, it risks making the victims of cybercrime bear disproportionate costs to prevent loss, while doing little to raise the costs to perpetrators. The IP Commission Report recommends several measures to increase the deterrent value of U.S. policy against cybercrime.

4. Strategy on Mitigating the Theft of U.S. Trade Secrets

In February 2013, the White House released its "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." The strategy has five main pillars:

1. international engagement, including diplomatic messaging and use of trade policy tools
2. company-to-company sharing of best practices to reduce the risk of trade secret theft
3. investigation and prosecution of trade secret theft and increased information sharing between law enforcement, the intelligence community, and companies,
4. a review of U.S. legislation,
5. increasing public awareness of the risks of trade secret theft.[3]

Although the strategy has many important components, its singular shortcoming is that it focuses almost exclusively on preventing loss from the perspective of the potential victim of trade-secret theft. The strategy does not address what ought to be done to raise the costs to the people and institutions that commit such theft. The IP Commission Report builds on this solid foundation by offering recommendations for substantive executive orders and legislative proposals that raise the costs of stealing U.S intellectual property and thus increase deterrence.

5. U.S. Capacity-Building Efforts in Foreign Countries

The May 2013 Special 301 Report by the U.S. Trade Representative also notes some important IP capacity-building efforts undertaken by the U.S. government:[4]

- The Global Intellectual Property Academy (GIPA) in the Office of Policy and External Affairs at the U.S. Patent and Trademark Office (USPTO) "offers programs in the United States and around the world to provide education, training, and capacity-building on IPR protection and enforcement. These programs are offered to patent, trademark, and copyright officials, judges and prosecutors, police and customs officials, foreign policymakers, and U.S. rights holders." The report adds that in 2012 "GIPA provided training to 9,217 foreign IPR officials from 130 countries, through 140 separate programs."
- The report notes that U.S. government agencies, such as the Department of State and the U.S. Copyright Office, "conduct conferences and training symposia in Washington, D.C. In March 2012, for example, the Copyright Office, with co-sponsorship from the World Intellectual Property Organization, hosted an international training symposium for representatives from

[3] Office of the U.S. Intellectual Property Enforcement Coordinator, "Intellectual Property Spotlight," January/February 2013, 1. For the text of the strategy, see Executive Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," 2013.

[4] The items in the following bulleted list are drawn from Office of the USTR, "2013 Special 301 Report," May 2013, 16–18, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

17 developing countries and countries in transition on emerging issues in copyright and related rights."

- In addition, "the USPTO's Office of Policy and External Affairs provides capacity building in countries around the world, and has concluded agreements with more than 40 national, regional, and international IPR organizations."
- Further, "the Department of Commerce's International Trade Administration (ITA) collaborates with the private sector to develop programs to heighten the awareness of the dangers of counterfeit products and of the economic value of IPR to national economies."
- In 2012, the Immigration and Customs Enforcement's Homeland Security Investigations conducted training programs overseas through the National IPR Coordination Center and in conjunction with INTERPOL.
- The Department of State "provides training funds each year to U.S. Government agencies that provide IPR enforcement training and technical assistance to foreign governments."
- The "government-to-government technical assistance" provided by the Commerce Department's Commercial Law Development Program is in large part focused on IPR protection.
- The Department of Justice's Criminal Division, which is funded by the Department of State, provided IPR-enforcement training to foreign officials in cooperation with other U.S. agencies.

Chapter 9

Developments in China

The IP Commission Report demonstrates through a variety of metrics that IP theft is a global problem but that Chinese-origin IP theft is disproportionately large in size and impact. Notwithstanding this evidence, it should be noted that China has made important strides in improving its IP protection.

China's patent system, in particular, has made progress, according to some measures. As chapter 4 observes, China now grants more patents than any other country (more than 1.6 million in 2011 alone). While many are utility or "petty" patents and of low quality, the process of granting patents reflects important steps along a road toward greater rule of law.[1] However, as chapter 4 also noted, the increase in patents largely represents a response to government incentives programs to patent rather than to innovate.

Other highlights of the Chinese system include better IP-enforcement and IP-protection strategies. Some important trends are worthy of highlighting in data made available from reporting on IP enforcement in 2012:

- In 2012, civil IP cases increased by nearly 50% to a total of 87,419 cases accepted. (This is more than five times the total of six years prior.)
- The courts accepted 7,840 criminal IP cases, an increase of more than 150% over 2011.
- Patent administrative appeals remained mostly static over previous years, suggesting that it is still difficult to appeal a decision of the State Intellectual Property Office.
- There were 420 specialized IPR tribunals in 2012. The number of basic courts that can hear IP cases increased from 29 in 2009 to 69 in 2012, but there was no change in the number of high courts engaged in the effort to combine civil, criminal, and administrative cases since 2009. However, China has nothing like the U.S. Court of Appeals for the Federal Circuit, which is an example of an appellate patent court.[2]

China's State Intellectual Property Office released its national IP strategy for 2013 in March 2013. Key elements of this ambitious plan include:[3]

- Prepare a work plan for intellectual property in China's strategic and emerging industries
- Prioritize patent examination for industries such as clean energy
- Improve statistical reporting on copyright, and prepare a report on the contribution of the copyright industries to China's economy
- Increase the number of basic courts hearing IP cases, the number of intermediate courts hearing patent cases, and the experiments in combining civil, criminal, and administrative IP cases
- Promote openness in administrative proceedings with model rules

---

[1] WIPO, Country Statistical Profiles (China), http://www.wipo.int/ipstats/en/statistics/country_profile/countries/cn.html.

[2] See "Supreme People's Court Annual Report Shows Continued Meteoric Growth in Litigation and Increasing Professionalism of the Court," China IPR, web log, April 25, 2013, available at http://wwwchinaipr.com.

[3] The following list draws from the "Promotion Plan for the Implementation of the National Intellectual Property Strategy in 2013," Office of the Inter-Ministerial Joint Meeting for Implementation of the National Intellectual Property Strategy, available at http://www.cipnews.com.cn/showArticle.asp?Articleid=26744.

- Improve coordination between administrative and criminal enforcement
- Promote software legalization by the government and preinstallation of legal software
- Improve patent administrative enforcement
- Conduct preparatory work for China to join the Hague Convention on industrial designs
- Enhance the protection of geographical indications, including at the border, and proceed with the negotiation of the Sino-European agreement on geographical indications
- Develop access and benefit-sharing rules for genetic resources
- Improve IP management in national science and technology projects, and develop new rules and practices for transgenic biotechnology, including new rules on IP protection
- Work to improve the situation for overseas students returning to China
- Continue efforts to increase IP-capable people in China, including a focus on textbooks for teaching the young, and begin to develop IP-service professions, including new regulations on patent and trademark agents and law firms handling patent matters

Supporters of developments in China make note of the "stage of economic development" dynamic for Beijing. They essentially argue that when China begins producing its own intellectual property in significant quantities, the country's own entrepreneurs and inventors will put pressure on political and Communist Party leaders to change the laws and improve IP protections. There is evidence that this is already happening.[4]

The Special 301 Report released in May 2013 by the U.S. Trade Representative notes some additional ways in which China's IP-protection system has made improvements.[5]

- On January 1, 2013, a new Chinese civil procedure law went into effect that might address some hurdles U.S. plaintiffs face in seeking redress in Chinese civil court actions.
- Also effective January 1, 2013, the Supreme People's Court issued a judicial interpretation on the liability of Internet intermediaries entitled "Rules of Supreme Court on Several Issues Concerning the Application of Law in Adjudication of Civil Disputes Related to Infringement of Right of Communication over Information Networks."
- China invited comment on numerous draft rules and guidelines for proposed regulations governing domestic IPR enforcement, suggesting a degree of willingness to hear foreign inputs.
- China's State Council established a permanent national leading group office (Leading Group) to better coordinate and improve the country's efforts to combat IP infringement and the manufacture and sale of counterfeit goods. Under the Leading Group, eleven special campaigns concentrating on key IP concerns were completed in 2012. This development is potentially of great importance.
- In May 2011, the Chinese government reported that software legalization in central government offices was complete. At the provincial level, a similar effort was reported to have been completed by the end of 2012. Software legalization efforts have more recently extended to Chinese state-owned enterprises (SOE). In 2012, China confirmed that it requires SOEs "to purchase and use legitimate software, including but not limited to operating system and office suite software."[6]

---

[4] USTR, "2012 Special 301 Report," April 2012, http://1.usa.gov/IkSucw.

[5] USTR, "2013 Special 301 Report," May 2013, 32–33, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

[6] Ibid., 34.

- China has made important commitments regarding technology transfer as well: "That technology transfer and technological cooperation shall be decided by businesses independently and will not be used by the Chinese Government as a pre-condition for market access," and "to treat and protect intellectual property rights (IPR) owned or developed in other countries the same as domestically owned or developed IPR." In addition, at the 2012 Joint Commission on Commerce and Trade, China "reaffirmed that technology transfer and technology cooperation are the autonomous decisions of enterprises" and further pledged that "if departmental or local documents contain language inconsistent with the above commitment, China will correct them in a timely manner."[7]

[7] USTR, "2013 Special 301 Report," 36.

Chapter 10

Short-term Solutions: Agile Administration Executive Action

The immediate actions we are recommending, largely regulatory or made effective via executive order, seek to provide immediate redress to a range of IP-theft problems.

Recommendation:

Raise the policy and enforcement priority of IP protection in the U.S. government. Designate the national security advisor as the principal policy coordinator for all actions regarding the protection of American intellectual property.

The position of the U.S. Intellectual Property Enforcement Coordinator, established by Congress in 2008, is currently a statutory office in the Office of Management and Budget. The office is staffed by U.S. government personnel mostly on detail from other enforcement agencies. The current coordinator is well respected, and her office is busy at the working level, yet the importance of the problem demands higher-level attention.

The theft of intellectual property poses enormous challenges to American national security and the welfare of the nation, as has been demonstrated in the preceding chapters. The risks include the possibility that theft of sensitive military or dual-use technologies can benefit potential adversaries. Other challenges extend to the potential degradation of the industrial base, in part from the sheer breadth and volume of attacks (see chapter 5). Although it is certainly true that not all problems rise to a national security challenge, the means by which IP is stolen (including foreign government involvement) and the recent assertion by the president's national security advisor that the U.S. government must take action to safeguard American companies in response to massive cyber and other attacks demonstrate that IP theft is a national security priority.[1]

The nature of the challenge is complex and broad in scope, with significant ramifications for bilateral relations with China and other major countries with which the United States has many common and conflicting interests. Therefore, the responsibility for interagency coordination must reside in the White House. Such a set of challenges requires the direct involvement of the president's principal advisor on national security issues to ensure that it is given the proper priority and the full engagement of the U.S. government.

While the Commission believes that policy coordination and emphasis on IP protection need to be accomplished at the White House level, it does not recommend that the detailed work of implementing an effective program can or should be supervised by White House staff. Efforts to protect American intellectual property will involve literally 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. The government needs to develop an interagency team of expert

[1] In his speech to the Asia Society in March 2013, the president's national security advisor, Thomas Donilon, made clear the linkage between attacks on American companies, especially via cyber means, and U.S. national security.

officials similar to, but even more active than, the Committee on Foreign Investment in the United States (CFIUS). Membership on the interagency team would include, at a minimum, representatives from the Commerce Department, FBI, Justice Department, Office of the Director of National Intelligence, State Department, U.S. Customs and Border Protection, U.S. Patent and Trademark Office, and U.S. Trade Representative.

Accomplishing all of these specific actions under a higher-priority IP-protection program will require the leadership of a cabinet-level official charged with sufficient responsibility.

Recommendation:

Establish the secretary of commerce as the principal government official responsible for enhancing and implementing policies regarding the protection of intellectual property, enforcement of implementation actions, and policy development.

The USTR has statutory authority to identify, monitor, and assess foreign countries for their protection of intellectual property and adherence to trade-agreement obligations. The USTR is principally and properly focused on the international trade environment. The Commission recognizes this important role for the USTR and seeks to complement it by strengthening the authority of the secretary of commerce to organize operational elements of the U.S. government to improve IP-protection measures.[2]

Despite the great work being done by the office of the USTR through the Special 301 Report and ongoing bilateral and multilateral negotiations, as well as increased enforcement efforts through the Office of the Intellectual Property Enforcement Coordinator, IP-related losses by U.S. companies appear to be getting worse. Chapter 1 discusses this and other problems with the current U.S. policy responses to the theft of IP by foreign actors.

The secretary of commerce has sufficient human, budget, and investigative resources to address the full range of IP-protection issues. The under secretary of commerce for intellectual property/director of the USPTO is already the president's advisor on intellectual property policy. Giving the secretary of commerce statutory authority for overall responsibility for implementation of IP policy builds on existing authorities and leverages the other existing capabilities within the Commerce Department.

The Commission recommends that an executive order be drafted that assigns the secretary of commerce the following responsibilities:

- Publication of an annual report describing the state of IP protection, including both overall numbers of violations and descriptions of major violations, as well as the effectiveness of U.S. IP-protection policy with recommendations to improve
- Responsibility for recommending to the secretary of homeland security the sequester of imported goods that have been judged to contain or benefit from stolen U.S. intellectual property
- Responsibility for recommending to the secretary of the treasury the sanctioning of individuals and companies that have stolen U.S. intellectual property

---

[2] The USTR's Special 301 Report states the following: "Pursuant to Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act ('Special 301'), USTR is required to identify those countries that deny adequate and effective protection for IPR or deny fair and equitable market access for persons that rely on IPR protection. The USTR is required to designate countries that have the most onerous or egregious acts, policies, or practices and whose acts, policies, or practices have the greatest adverse impact (actual or potential) on the relevant U.S. products as "Priority Foreign Countries. USTR has created a 'Priority Watch List' and 'Watch List' under Special 301 provisions. Placement of a trading partner on the Priority Watch List or Watch List indicates that particular problems exist in that country with respect to IPR protection, enforcement, or market access for persons relying on IPR." Office of the United States Trade Representative, "2013 Special 301 Report," May 2013, 57, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

- Responsibility for developing and chairing an interagency team of expert officials from all involved departments to develop a detailed body of knowledge on the full extent of foreign misappropriation of U.S. intellectual property, and to recommend counter-employing the full range of official sanctions

Recommendation:

Establish a quick-response capability to sequester imported goods that incorporate stolen or pirated materials or were made with a business process that includes illegally procured intellectual property, strengthening the existing 337 process of the Tariff Act.

The example of thousands of counterfeit parts arriving on U.S. shores, as discussed in chapter 1, and the increasing use of the international mail system to send trademark-infringing goods into the United States, highlighted in chapter 6, both point to a need to provide a faster process to identify and sequester goods entering the U.S. market from abroad.

While faster than federal court litigation, the current USITC sequestration process pursuant to Section 337 of the Tariff Act of 1930 is still too lengthy and bureaucratic to protect American companies that find their products or processes infringed upon by goods entering the United States. Under current practice, a case is not accepted by the USITC unless a lengthy complaint is submitted. Moreover, after an investigation (of unbounded duration) if the administrative law judge assigned to the case supports a finding of IP violations, a judgment preventing goods from entering the U.S. market takes effect 60 days after the judgment. Average case time is more than a year. While provisions for temporary relief exist, the rules emphasize compliance above stopping illegal use of the intellectual property of others.[3]

As mentioned in chapter 1, the profitable life cycle of certain goods is strongest in the immediate days and weeks following the product's release. In this context, the existing Section 337 process does not provide a rapid enough mechanism for companies to seek injunctions and compensation for infringement. In an era in which the profitable life cycles of some goods and processes can be measured in days and weeks, the existing Section 337 process is in desperate need of overhaul.

What is needed is a faster process that can sequester goods suspected of containing illegally obtained IP (under a "probable cause" standard of proof) until rapid judgment can be made that the goods or processes contain no illegal IP. Once the judgment is made, then the company's export license for those goods is revoked if the presence of illegal IP is confirmed, or the goods are released for import if no infringement of IP is confirmed.

For this recommendation, the sequestration would be triggered either by U.S. government information or by information provided by companies as they scan their own markets. The government team described below must ensure that the procedures for a U.S. company to trigger a complaint are not so burdensome that small and medium-sized U.S. companies are discouraged from using them. If lengthy procedures become necessary, then the government team needs to establish a "help desk" to assist smaller companies in submitting complaints.

Once theft of a product or process is alleged, the interagency team described above would consider the case under an expedited deadline. This process would set a lower standard of proof for the merits of the allegation, a standard similar to the "probable cause" used for the issuance of warrants to law-enforcement officers to make searches, on the premise that speed is the most important dimension

[3] USITC, "Section 337 Investigations: Answers to Frequently Asked Questions," March 2009, http://www.usitc.gov/intellectual_property/documents/337_faqs.pdf.

in limiting losses to rights holders. An expedited legal review would then ensue within a strict time frame to determine whether to keep the goods impounded or allow them to enter the U.S. market.

American businesses consider a "bar to entry" dimension to be an essential component of a broad-based IP-enforcement program, as it serves to prevent economic harm to American companies from occurring while a careful review of a product is undertaken. Restricting the entry of IP-invalid goods or services both protects the market share of IP-compliant companies and conveys a powerful deterrent message to potential violators. A mandatory legal review ensures that the rights of companies entering the U.S. market are protected. Evidence from a study by the *Michigan Law Review* finds that default rates are rising faster than the increase in USITC 337 cases in recent years, thereby keeping counterfeit goods from the American market. This trend suggests that in many cases the mere threat of a USITC investigation serves the deterrent purposes of preventing counterfeit goods from entering the U.S. market.[4]

This recommendation has two potential negative effects that must be monitored and, if necessary, mitigated. Companies found not to be in violation could, in some cases, sue the U.S. government for loss of revenue. A swift and transparent adjudication process should mitigate this potential effect. Another potential downside of this process is that it could create a perverse incentive for American companies to lodge false allegations against foreign competitors as a means to gain a short-term advantage. The interagency team that accepts and evaluates complaints will quickly learn whether the system is being manipulated and can easily decline to accept additional complaints from these American companies.

While this process would have no effect on goods or processes that do not enter the U.S. market, it will have a strong deterrent effect on major foreign companies with international ambitions, as it forces them to choose between obtaining IP illegally and selling in the U.S. market. This quick-response capability is based on identification of a particular good or service that incorporates stolen IP. The penalty for the infraction is taken against the product or service. When a Chinese or other foreign company is identified as a repeat offender, using stolen IP on a larger scale, then action needs to be taken against the company itself.

Recommendation:

Empower the secretary of the treasury, on the recommendation of the secretary of commerce, to deny the use of the American banking system to foreign companies that repeatedly benefit from the misappropriation of American intellectual property.[5]

Foreign companies that sell goods or services in the American market, or do business in dollar-denominated markets, such as the international oil market, must use American banks to clear their transactions. Chapter 1 discusses how companies may illegally make use of the IP of American companies as part of their supply chains, and chapters 6 and 7 discuss misappropriation of IP through trademark and copyright infringement. Companies that repeatedly misappropriate the intellectual property of an American company—either as incorporated within their product or as part of the business process (machine tools, business software, etc.) that created the good or service—should forfeit the privilege of using the American banking system.

---

[4] John C. Evans, "Addressing Default Trends in Patent-Based Section 337 Proceedings in the United States International Trade Commission," *Michigan Law Review* 106, no. 4 (2008).

[5] Using the language "use or benefit from" implies a broader reach. It includes not only the thieves of the IP but also those who, for example, have licensed IP but use it past the expiration of the license or use it for a purpose that is not covered by the license.

International banks are the gateway to the American economy. Banking restrictions have proved to be an extremely effective tool in controlling financial operations related to other illegal international activities, such as terrorism, money laundering, and drug smuggling. Making compliance with IP laws a prerequisite for entry into the U.S. market, and utilizing the financial system as the gatekeeper of that process, creates an enforcement tool without geographical boundaries. Companies that make use of stolen American IP anywhere in the world would suddenly face the real prospect of severe restrictions on their ability to access the U.S. banking system.

The same Commerce-led interagency team established in the recommendations above would have the expertise, experience, and charter to determine which foreign companies should be subject to this sanction. When the interagency team observes repeated confirmed instances of IP theft by a foreign company, it would forward the name of that company to the secretary of the treasury for financial sanctions for a period of time.

The Commission does not prescribe specific lengths of time for the sanction to be imposed, nor procedures for a foreign company to be removed from the sanctions. These procedures should be at the discretion of the interagency team, based on its experience. The Commission is fairly certain that, unlike in the cases of terrorist financing that supports ideologically driven mayhem or inherently illegal activities such as drug-smuggling or money-laundering, using American financial institutions to sanction market-sensitive enterprises that steal IP would have enormous deterrent value. The number of companies that are stealing IP would likely dwindle rapidly.

Chinese or other foreign companies may resort to tactics such as the use of "reverse mergers" and the creation of shell companies and subsidiaries to protect parent companies from these financial sanctions. The interagency team would thus need to establish procedures to ensure that the penalties affect the parent company.

This recommendation would add one more set of administrative requirements and open one more potential basis for suits to the already heavy burdens placed on American international banks. On the other hand, it establishes no new processes or mechanisms to the existing requirements for understanding their customers, which ensure that U.S. banks are not being used for other forms of illegal activity. Foreign companies and governments may consider bringing action against the United States in the WTO for these procedures, but the Commission believes that this is a risk worth taking.

Recommendation:

Increase Department of Justice and FBI resources to investigate and prosecute cases of trade-secret theft, especially those enabled by cyber means.

While issues of IP protection are not necessarily new, as the Commission and this report point out, what has changed dramatically in recent years is the way in which new capabilities, such as cyber, have affected and enabled the stealing of trade secrets. The discussion in chapter 1 of cyber methods sets the background for the importance of this recommendation.

The Department of Justice and FBI need more resources to investigate the sharp increase in trade-secret theft cases, and the Commission strongly recommends the increase of investigative and prosecutorial resources. These resources are especially needed to investigate cases where the theft was perpetrated against small businesses and start-ups, as mentioned in chapter 1. Start-ups and small businesses are an indispensable part of the United States' culture of innovation, are being increasingly targeted by IP thieves, and have fewer resources to defend themselves.

Recommendation:

Consider the degree of protection afforded to American companies' IP a criterion for approving major foreign investments in the United States under the Committee on Foreign Investment in the U.S. process.

CFIUS is an interagency committee authorized to review transactions that could result in control of a U.S. business by a foreign entity in order to determine the effect of such transactions on the national security of the United States. If CFIUS finds that a covered transaction presents national security risks and that other provisions of law do not provide adequate authority to address the risks, then CFIUS may enter into an agreement with or impose conditions on parties to mitigate such risks or may refer the case to the president for action.[6]

As demonstrated by the flood of counterfeit parts discussed in chapter 1, as well as by widespread cyber infiltrations discussed in chapters 1 and 5, the Commission assesses that the theft of American intellectual property has direct implications for national security. Given that CFIUS has a large amount of flexibility in evaluating potential transactions, it seems appropriate for CFIUS to factor into its judgment the degree to which the foreign actor protects intellectual property.

Recommendation:

Enforce strict supply-chain accountability for acquisitions by U.S. government departments and agencies by June 1, 2014, and work to enhance corporate accountability for the IP integrity of the supply chain.

Chapter 1 discusses the ways in which companies that use illegal IP as part of their supply chain, either as a process or part of an end product, gain an unfair advantage in the marketplace against those who are careful to audit and patrol their suppliers and factories. The U.S. government should not be giving business to contractors that use stolen IP in the goods and services they provide, including their subcontractors and subcomponents. Governments traditionally have imposed heightened requirements on contractors on the rationale that taxpayer funds should not be used to support businesses that engage in unethical or illegal conduct.

At least with regard to software, legal bases currently exist to impose IP compliance requirements on federal contractors. Executive Order 13103, signed by President Clinton on September 30, 1998, requires not only that federal agencies use legal software in their own operations, but also that they impose similar requirements on contractors:

> Contractors and recipients of Federal financial assistance, including recipients of grants and loan guarantee assistance, should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. If agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors or recipients may affect the

[6] "CFIUS operates pursuant to section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 (FINSA) (section 721) and as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Part 800… The members of CFIUS include the heads of the following departments and offices: Department of the Treasury (chair); Department of Justice; Department of Homeland Security; Department of Commerce; Department of Defense; Department of State; Department of Energy; Office of the U.S. Trade Representative; and Office of Science & Technology Policy. The Office of Management & Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council are observers. The Director of National Intelligence and the Secretary of Labor are non-voting, *ex-officio* members of CFIUS with roles as defined by statute and regulation." See U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," December 20, 2012, http://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx.

> integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law.

Other provisions of U.S. procurement law provide additional bases for requiring federal contractors to use legal software. The Federal Acquisition Regulation (FAR), which governs most federal contracts, requires contracts expected to exceed $5,000,000 and a performance period of 120 days or more to include a clause requiring the contractor to comply with applicable laws and generally adhere to ethical business practices.[7] Similarly, contracts for the acquisition of commercial items must contain the clause at FAR 52.212-4, *Contract Terms and Conditions—Commercial Items*, one provision of which provides that contractors "shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract."[8]

Federal agencies should enforce Executive Order 13103 more aggressively, including by requiring contractors to certify that they comply with the order as a condition of bidding on federal contracts. Federal agencies also should interpret Executive Order 13103's provision prohibiting contractors from using federal funds to acquire, operate, or maintain unlicensed software to bar the use of unlicensed software throughout the contractor's business operations. Consideration should be given to applying the same rules to subcontractors.

Additionally, organizations such as CREATe and Verafirm have developed processes that assist companies with increasing the accountability of their supply-chain providers.[9] Companies can be held accountable through their supply chains for certain marine content in fish products, textiles produced by minors, and toxic materials in consumable products. Thus, these companies can be held accountable for ensuring that the supply chains and processes they oversee are also IP-protection compliant.

Beyond its recommendations for the U.S. government, the Commission encourages businesses to improve their audits and accountability for their own supply chains. Corporate executives should be encouraged to adopt a zero-tolerance policy toward IP theft within their companies and with their suppliers, including foreign suppliers, and to consider a mechanism whereby the company can be alerted about known or suspected IP theft, including in their supply chains. Companies also should seek to implement best practices with regard to supply-chain IP compliance. Specifically, companies should implement audit provisions in supply-chain agreements requiring suppliers to increase accountability.

Over time, what could develop is a process whereby an IP certification, or "IP passport," could be awarded to companies with a high degree of integrity in their international supply chains. This would have demonstrable benefits for the speed with which the goods and services enter the U.S. market.

The Commission acknowledges that for some small and medium-sized enterprises increasing accountability in supply chains can pose a burden. However, the Commission also notes that increasing such protection actually improves the legal standing of companies in the event of lawsuits.

---

[7] See Federal Acquisition Regulation §3.1004(a), requiring use of contract clause at §FAR 52.203-13, *Contractor Code of Business Ethics and Conduct*, which require contractors to "promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law," to have an internal control system that establishes "standards and procedures to facilitate timely discovery of improper conduct in connection with Government contracts," and to impose "disciplinary action for improper conduct or for failing to take reasonable steps to prevent or detect improper conduct."

[8] 48 CFR 52.212–4(q).

[9] See CREATe, "Tools and Training," http://www.create.org/tools-training; and Verafirm, "About Verafirm," https://www.verafirm.org/Pages/General/About.aspx.

Recommendation:

Require the Securities and Exchange Commission (SEC) to investigate whether the knowing, systematic, or widespread use of stolen software or other stolen IP within a listed company is or should be subject to executive and auditor disclosure rules and, if so, to issue guidance to that effect (a "red flag" provision).

Chapter 1 describes the degree to which supply chains are an increasing source of IP theft. Further targeting the misappropriation of IP in globalized supply chains, the SEC can play a significant role as a watchdog with regard to U.S.-listed companies. In recent years, U.S. policymakers and regulators have become increasingly active in requiring publicly listed companies to promote legal compliance and root out fraud. This is based in part on the rationale that a corporate culture that tolerates legal violations and fraud is more likely to engage in conduct that could mislead investors about the company's financial health.

An example of this can be found in Section 302 of the Sarbanes-Oxley Act. The SEC rules for implementing Section 302 require the CEO and CFO of a listed company (including a foreign private issuer) to disclose any fraud to the company's auditors and board of directors, whether or not material, that involves management or other employees who have a significant role in the company's internal control over financial reporting.[10] Failure to act on known fraud may subject the CEO and CFO to personal liability, which could extend to board members in certain cases.

Separately, the Securities Exchange Act provides that if a company's auditors become "aware of information indicating that an illegal act (*whether or not perceived to have a material effect on the financial statements of the company*) has or may have occurred," the auditor must inform "the appropriate level" of the company's management and insure that the company's audit committee—or board of directors in the absence of an audit committee—is "adequately informed with respect to illegal acts" that the auditor has detected.[11] A company's use of stolen software falls within the scope of this provision, yet most auditing firms today do not routinely audit listed companies for legal software use.

The Commerce-led interagency team proposed in the two previous recommendations will also have information that should be provided to the SEC to be used in the regulation of both companies that are currently listed on American stock exchanges and those that are applying for listing.

There is ample evidence that stolen software can introduce security vulnerabilities into a company's IT system.[12] Use of such software within a corporation is a "red flag" of inadequate internal controls more broadly. If the SEC makes such a finding, it should work with other international securities regulators to implement a standardized approach.

Recommendation:

Greatly expand the number of green cards available to foreign students who earn science, technology, engineering, and mathematics (STEM) graduate degrees in American universities.

Chapter 1 highlights the issue of highly skilled foreign students who are unable to stay in the United States after graduation due to U.S. government limitations on visas. According to a recent

---

[10] Securities Exchange Act of 1934, rules 13a-14, 15d-14.

[11] Securities Exchange Act of 1934, §10A(b)(1).

[12] See John F. Gantz et al., "The Dangerous World of Counterfeit and Pirated Software: How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations…and the Resultant Costs in Time and Money," IDC, White Paper, no. 239751, March 2013, 3–4, http://www.computerworld.com.pt/media/2013/03/IDC030513.pdf.

Brookings Institution study, in 2010 more than 96,000 foreign students were in the United States pursuing graduate degrees in STEM fields. However, a mere 19,000 stayed after graduation to work in the United States. Many American high-tech companies have publicly advocated increasing the number of visas available for these scientists and engineers in order to help them fill open jobs. However, the loss of these valuable workers has other damaging effects. Many of the 77,000 graduates who return home every year have knowledge of American intellectual property, gained in the course of their studies or in internships during their time in the United States. This intellectual property is of great benefit to foreign companies, enabling them to more quickly and effectively compete with American companies, both in overseas markets and even in the American market.

Several proposals to reform U.S. immigration procedures would make earning a green card for graduate students in STEM fields an easier process after graduation and with a job offer in hand. The Brookings study estimated that numerous metropolitan areas, especially in the Midwest, would see dramatic benefits if a much larger percentage of foreign students were permitted to stay.[13]

The Commission supports such initiatives on immigration reform. Sending qualified and talented scientists and engineers home almost ensures that their American educations will benefit other nations' economic development and will represent missed opportunities for the American economy.

To be sure, some of the foreign students who would remain in the United States under the terms of this arrangement would be subject to pressure or inducements from home countries and companies to commit IP theft while working for a U.S. company. There have been multiple cases of the FBI prosecuting green card holders. Nonetheless, if the full range of this report's recommendations were adopted to deal with IP theft systemically, the Commission judges that this risk is far outweighed by the potential benefits of such a program.

[13] Neil Ruiz, "Immigration Facts on Foreign Students," Brookings Institution, April 9, 2013, http://www.brookings.edu/research/interactives/2013/facts-on-foreign-students.

Chapter 11

Medium-term Solutions: Legislative and Legal Reform

These are efforts that will strengthen the U.S. legal system, which possesses inadequate legal remedies for the scale of the problems we face, and increase the priority of IP protection in U.S. diplomatic missions overseas.

Recommendation:

Amend the Economic Espionage Act to provide a private right of action for those who hold trade secrets and further to make the Court of Appeals for the Federal Circuit (CAFC) the appellate court for all actions under this statute.

The EEA was passed in 1996 to criminalize trade-secret theft at the federal level in order to provide a mechanism to stem losses to U.S. entities as a result of such theft. Two amendments recently signed into law by President Obama serve to broaden the scope of protection (Theft of Trade Secrets Clarification Act of 2012) and to increase monetary penalties for criminal activities under the EEA (Foreign Economic Espionage Penalty Enhancement Act of 2012).

As discussed in depth in chapter 5, while the EEA has been somewhat helpful in protecting IP internationally, there are still some deficiencies that need to be addressed. Missing from the EEA is a private civil cause of action that would enable companies to individually pursue the perpetrators of economic espionage in federal court, though the statute does create a limited civil cause of action allowing the U.S. attorney general to seek injunctive relief against offenders. Under current law, companies and individuals are left to pursue their cases for trade-secret misappropriation in state courts, which gives rise to many of its own complications, including limited access to evidence and difficulty in enforcing judgments.[1]

An amendment allowing a private civil cause of action under the EEA would allow the rights holders themselves, rather than just government prosecutors, to file lawsuits in order to protect their proprietary methods and information. This could also help alleviate the burden on federal prosecutors, who are already suffering from severe resource constraints when it comes to pursuing EEA actions.

---

[1] A bill that would have provided a private civil cause of action at the federal level for economic espionage was introduced in July 2012, entitled the Protecting American Trade Secrets and Innovation Act of 2012. The bill would have amended §1836 of the EEA to allow a person who is aggrieved by an act of economic espionage, theft of a trade secret, or misappropriation of a trade secret that is related to or included in a product that is produced for or placed in interstate or foreign commerce to bring a civil action under the EEA, instead of requiring that the civil action be brought by the U.S. attorney general.

As summarized by the Library of Congress, the bill contained the following provisions: "Requires a complaint filed in such an action to: (1) describe with specificity the reasonable measures taken to protect the secrecy of the alleged trade secrets in dispute, and (2) include a sworn representation by the party asserting the claim that the dispute involves either substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country. Authorizes the court, in a civil action, upon ex parte application and if the court finds by clear and convincing evidence that issuing the order is necessary to prevent irreparable harm, to issue an order providing for: (1) the seizure of any property (including computers) used or intended to be used to commit or facilitate the commission of the alleged violation, and (2) the preservation of evidence. Sets forth provisions regarding the scope of such an order, rights of a party injured by a seizure under such an order, and remedies with respect to civil actions brought under this Act. Establishes a three-year limitations period, beginning when the misappropriation is discovered or should have been discovered." See Library of Congress, "Summary: S.3389—112th Congress (2011–2012)," available at http://beta.congress.gov/bill/112th%20Congress%20(2011-2012)-congress/senate-bill/3389.

The second proposed change to the Economic Espionage Act mandates that the appellate court for all actions under the EEA would be the Court of Appeals for the Federal Circuit. The CAFC serves as the appellate court for nearly all IP-related cases, and thus has a high degree of competency on IP issues. Making the CAFC the appellate court for all EEA issues ensures a degree of continuity in judicial opinion. Moreover, it helps support the federal circuit in expanding extraterritorial enforcement.

Recommendation:

The U.S. Federal Trade Commission (FTC) should investigate instances of foreign companies stealing IP and use its broad enforcement powers under Section 5 of the FTC Act to obtain meaningful sanctions against any foreign companies that use stolen IP. The Commission also recommends that attorneys general of other states follow the example of the recent aggressive enforcement actions against IP theft taken by the California and Massachusetts attorneys general.

Most businesses today rely on software and other information technologies to improve their efficiency and productivity. In a 2008 study, the U.S. Department of Commerce found a significant correlation between IT investment and productivity growth.[2] In 2010, U.S. manufacturers spent nearly $30 billion on software in order to run their businesses more efficiently and to gain a competitive edge.[3] Many of these companies operate on tight margins where small differences in costs can significantly affect their profits and market success.

When a foreign company uses stolen software to run its business and then competes in a U.S. market against companies that use legal software, this distorts competition in the United States by providing the foreign company with an unfair and artificial cost advantage. If left unaddressed, this creates perverse incentives by providing a competitive advantage to companies that engage in illegal conduct and placing at a competitive disadvantage those law-abiding companies that may be more innovative or efficient but that pay for their software. These market distortions may reduce lawful competition and lead to suboptimal investments in innovation, since enterprises that pay for their software and lose sales to firms that engage in software theft will have fewer resources to invest in R&D. Over time, software theft by foreign companies whose products or services are offered in U.S. markets will distort competition in these markets and will leave U.S. consumers worse off. Reiterating the earlier notions of chapter 1, these losses are becoming more and more potent due to shorter product life cycles. In industries that gain the vast majority of their revenues during the first few months of a product release, the enforcement mechanisms need to be equally responsive.

Legislatures in Washington State and Louisiana have passed laws specifically targeting this form of unfair competition,[4] while state attorneys general in California and Massachusetts recently announced actions against foreign manufacturers' use of stolen software under these states' respective

---

[2] According to the Department of Commerce, "average growth for IT-intensive industries for this period [1989–2001] was 3.03 percent, far exceeding growth in the less IT-intensive industries which averaged 0.42 percent." U.S. Department of Commerce, Economics and Statistics Administration, *Digital Economy 2003*, December 2003, 45–54, http://www.esa.doc.gov/sites/default/files/reports/documents/dig_econ_2003.pdf.

[3] Ben Law, Ted Dangson, and Stephen Minton, "United States Black Book: State IT Spending by Vertical Market—2Q11," IDC, September 2011.

[4] 2011 Wash. Leg. Serv. Ch. 98 (codified at Wash. Rev. Code §§ 19.330.010–100); and 2010 La. Sess. Law Serv. Act 74 (codified at La. Rev. Stat. § 51:1427).

existing unfair-competition laws.[5] Also, 39 state and territorial attorneys general recently sent a letter to the FTC highlighting the problem, pledging to seek ways to use the powers of their respective offices to address the issue, and urging the FTC to consider how Section 5 of the FTC Act could be brought to bear on the problem at the federal level.[6]

This recommendation is a complement to enacting a federal private right of action under a revised EEA. At the state level, the accumulation of case law will serve as a longer-term deterrent to illegal gain as a result of the misappropriation of intellectual property. State case law also extends to the unlawful use of pirated software in the production of a good. The Massachusetts attorney general recently brought a successful case against a Thai company, which settled out of court after paying a fine.[7]

Recommendation:

Expand and strengthen diplomatic priorities in the protection of American intellectual property by increasing the diplomatic rank of IP attachés assigned to priority embassies and by making the protection of intellectual property one of the criteria on which ambassadors are graded.

In countries with which the United States has a particularly challenging relationship in the field of IP protection, one way the United States can demonstrate the priority with which it holds the protection of intellectual property is by giving appropriately senior rank to its IP attaché. By doing so, the United States also facilitates more effective interactions with host countries and will contribute to more mature rule of law perspectives in many developing nations, as discussed in chapter 1.

Similarly, if the criteria on which U.S. ambassadors are evaluated on an annual basis include their efforts to protect American intellectual property, as they now include efforts to promote American exports, they would likely find new and innovative ways to protect IP. Moreover, adopting this recommendation will send a strong message to the host country.

---

[5] Commonwealth of Massachusetts, Attorney General's Office, "Company Fined for Using Pirated Software to Gain Unfair Advantage Over Massachusetts Businesses," Press Release, October 18, 2012, http://www.mass.gov/ago/news-and-updates/press-releases/2012/2012-10-18-narong-seafood-co.html; and State of California Department of Justice, Office of the Attorney General, "Attorney General Kamala D. Harris Files Unfair Competition Lawsuits Over Use of Pirated Software in Apparel Industry," Press Release, January 24, 2013, http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-unfair-competition-lawsuits-over-use.

[6] National Association of Attorneys General to FTC Commissioners and the Director of the Bureau of Competition, Washington, D.C., November 4, 2011, http://www.naag.org/assets/files/pdf/signons/FTCA%20Enforcement%20Final.PDF.

[7] Marjorie Nesin, "Fish Company Pays AG's fine for IT Piracy," *Gloucester Daily Times*, October 22, 2012, http://www.gloucestertimes.com/local/x1684128598/Fish-company-pays-AGs-fine-for-IT-piracy.

Chapter 12

Long-term Solutions: Capacity-building

This set of recommendations is aspirational in nature. The recommendations seek to build consensus in priority countries for the support of IP protection.

Recommendation:

Help build institutions in priority countries that contribute toward a "rule of law" environment in ways that protect intellectual property.

Currently, there is a range of efforts, both public and private, that contributes to the development of rule of law in China and other foreign countries that do not protect intellectual property. These should be encouraged and endorsed by Congress and the administration as extremely cost-effective ways to bring about systemic change.

In particular, the U.S. Patent and Trademark Office organizes a range of capacity-building efforts, such as U.S.-China legal exchanges, which include the participation of sitting American judges. These efforts are largely cost-free to taxpayers—being funded by the fees that the USPTO collects—and have been enormously effective. Of particular importance are efforts that demonstrate the purposes and value of an independent judiciary.

Recommendation:

Develop a program that encourages technological innovation to improve the ability to detect counterfeit goods and products.

The U.S. government has become quite good at motivating developments in the government and private sectors through a range of incentive programs. Such programs are often quite successful at developing new technological solutions that can have important policy impacts.

Innovation for the purposes of greater protection against counterfeiting also sends important messages about the value the U.S. government places on domestic innovation. Technologies that could more simply and reliably detect counterfeit items or verify the authenticity of true products are examples. Such an initiative is also self-reinforcing: innovation that protects existing innovation is thus both a goal and a means to an end.

Recommendation:

Ensure that top U.S. officials from all agencies push to move China, in particular, beyond a policy of indigenous innovation toward becoming a self-innovating economy.

As discussed in chapter 1, China in particular needs to continue to reform its IP-protection system. It is assessed that China will become a stronger supporter of intellectual property when Chinese innovators demand more domestic protection for their own technological advances. Chinese inventors and entrepreneurs are on the cusp of tremendous breakthroughs in a range of sectors. What they lack are the legal and regulatory protections at home that will enable them to realize the benefits of their ideas.

Bringing to an end the use of Chinese-granted "petty patents," as described in chapter 4, would be an important early step toward becoming an innovation economy. The system of petty, or utility, patents does not advance China toward becoming a technological leader. Quite the contrary, petty patents actually impede innovation because the system incentivizes the copying of others' work.

Recommendation:

Encourage the development of IP "centers of excellence" on a regional basis within China and other priority countries.

Incentivizing provincial and municipal leaders in countries such as China, Russia, and India to create business environments that protect intellectual property is a critical long-term activity. One of the ways the U.S. government can encourage better protection of intellectual property in China is pointing foreign investment toward those cities and provinces with stronger protection of intellectual property. Increased levels of foreign investment would then have positive impacts on helping reach the levels of economic growth that mark outstanding local leaders as destined for promotion.

This can be an enormously challenging process, especially in countries that have uneven IP-protection regimes in place. Developing a nongovernmental assessment and rating system, as described below, is a first step toward encouraging the development of IP centers of excellence.

Recommendation:

Establish in the private, nonprofit sector an assessment/rating system of levels of IP legal protection, beginning with China but extending to other countries as well.

The assessment would focus on the regional or sub-national level and could be conducted by an international consortium of relevant educational and business associations to provide both a status report and a directional indicator—improvement or regression—of the level of IP protection within a specific region. Such an assessment system would help identify geographical regions in which IP protection is notably stronger than in others. Implicit within the development of such a system is that foreign investors would use its findings to inform their own investment patterns in IP protection–challenged countries such as China, Russia, and India.

Chapter 13

Cyber Solutions

There are two types of intruders into corporate computer networks that are connected to the Internet. The "opportunistic hacker" uses the Internet to run probing attacks against many networks and then intrudes wherever he finds vulnerability. The "targeted hacker" seeks to take specific proprietary information in a specific network belonging to a specific government agency or private company. Whereas some hackers target entities for individual ideological reasons, many others are sponsored by a government agency, often for direct military purposes—intelligence and reconnaissance—or to damage military networks. Other targeted hackers seek to intrude on behalf of a foreign corporate competitor into the network of a U.S. corporation, often to take specific information to gain a business advantage. Cyberattacks, in combination with traditional economic espionage activities involving human efforts targeted against corporate proprietary information, can result in the theft of highly protected trade secrets.

The sheer scale of cyberattacks on American companies, with corresponding economic interests at stake, causes the issue of IP to rise to a genuine national security concern. The administration recognizes this new reality. As National Security Advisor Tom Donilon said recently, "the United States will do all it must to protect our national networks, critical infrastructure, and our valuable public and private sector property."[1]

Vulnerability Mitigation Is Effective Only against Opportunistic Hackers

Almost all network security approaches to date have been based on the concept of vulnerability mitigation, which seeks to strengthen one's existing network security by pursuing the newest and best software, network appliances, regular updates, updated firewalls, most recent patches to software weaknesses, and so forth. Moreover, they place a high burden on network administrators to comply with established minimum requirements and manage the integration of an ever-expanding universe of security products. Vulnerability mitigation is a fundamentally passive approach to network defense. Companies spend inordinate amounts of money attempting to protect their networks against all threats, but in reality only succeed in keeping out the opportunistic hackers who may otherwise have no direct interest in the information of a particular company. Thus, the costs borne by individual companies to defend themselves have no effect on the incentives of opportunistic hackers. Time and opportunity are on their side. If presented with a challenging network defense, they simply move on to more lightly defended networks. *Perhaps more importantly, vulnerability-mitigation measures have proved largely ineffective in defending against targeted hackers, who are hired specifically to pursue American corporations' intellectual property.*

A different concept for security, known as threat-based deterrence, has been identified as a means to protect the most important information in corporate or government networks.

[1] Thomas Donilon, "The United States and the Asia-Pacific in 2013" (speech to the Asia Society, New York, March 11, 2013), http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

Threat-based Deterrence against Targeted Hackers

Even the best security systems using vulnerability-mitigation measures, including those with full-time dedicated operations centers, cannot be relied on for protection against the most highly skilled targeted hackers. A network exists in order to share information with authorized users, and a targeted hacker, given enough time, will always be able to penetrate even the best network defenses.

Effective security concepts against targeted attacks must be based on the reality that a perfect defense against intrusion is impossible. The security concept of threat-based deterrence is designed to introduce countermeasures against targeted hackers to the point that they decide it is no longer worth making the attacks in the first place. In short, it reverses the time, opportunity, and resource advantage of the targeted attacker by reducing his incentives and raising his costs without raising costs for the defender. Conceptual thinking about and effective tools for threat-based deterrence are in their infancy, but their development is a very high priority both for the U.S. government and for private companies.

Chapter 1 provides an in-depth review of the extent to which cyberattacks affect the U.S. national economy, and chapter 5 discusses the problem of cyberespionage in detail.

Recommendation:

Encourage adherence to best-in-class vulnerability-mitigation measures by companies and governments in the face of an evolving cybersecurity environment.

Despite their limited utility against skilled and persistent targeted hackers, computer security systems still need to maintain not only the most up-to-date vulnerability-mitigation measures, such as firewalls, password-protection systems, and other passive measures. They should also install active systems that monitor activity on the network, detect anomalous behavior, and trigger intrusion alarms that initiate both network and physical actions immediately. This is a full-time effort. Organizations need network operators "standing watch" who are prepared to take actions based on the indications provided by their systems, and who keep a "man in the loop" to ensure that machine responses cannot be manipulated. Organizations need to have systems—software, hardware, and staff—to take real-time action to shut down free movement around the house, lock inside doors, and immobilize attackers once the alarms indicate that an intrusion has started. Some government agencies and a few corporations have comprehensive security systems like this, but most do not.

Finally, emphasis should be given to developing cutting-edge technologies that will promote a healthier Internet ecosystem. Examples of such technologies come in many forms. For one, since a large number of the successful targeted attacks are still arriving in the form of email campaigns containing links or files exploiting a zero-day vulnerability in common software packages, systems that are capable of rapidly analyzing the behavior of unknown files and links are an important element. So too is technology that allows for the isolation of computing environments so that damage is limited to a quarantined area and cannot infect the rest of the network. Last, systems providing advanced, real-time network analysis would also be a necessary element of this ecosystem.

Recommendation:

Support efforts by American private entities both to identify and to recover or render inoperable intellectual property stolen through cyber means.

Some information or data developed by companies must remain exposed to the Internet and thus may not be physically isolated from it. In these cases, protection must be undertaken for the files themselves and not just the network, which always has the ability to be compromised. Companies should consider marking their electronic files through techniques such as "meta-tagging," "beaconing," and "watermarking." Such tools allow for awareness of whether protected information has left an authorized network and can potentially identify the location of files in the event that they are stolen.

Additionally, software can be written that will allow only authorized users to open files containing valuable information. If an unauthorized person accesses the information, a range of actions might then occur. For example, the file could be rendered inaccessible and the unauthorized user's computer could be locked down, with instructions on how to contact law enforcement to get the password needed to unlock the account. Such measures do not violate existing laws on the use of the Internet, yet they serve to blunt attacks and stabilize a cyber incident to provide both time and evidence for law enforcement to become involved.

Recommendation:

Reconcile necessary changes in the law with a changing technical environment.

When theft of valuable information, including intellectual property, occurs at network speed, sometimes merely containing a situation until law enforcement can become involved is not an entirely satisfactory course of action. While not currently permitted under U.S. law, there are increasing calls for creating a more permissive environment for active network defense that allows companies not only to stabilize a situation but to take further steps, including actively retrieving stolen information, altering it within the intruder's networks, or even destroying the information within an unauthorized network. Additional measures go further, including photographing the hacker using his own system's camera, implanting malware in the hacker's network, or even physically disabling or destroying the hacker's own computer or network.

The legal underpinnings of such actions taken at network speed within the networks of hackers, even when undertaken by governments, have not yet been developed. Further, the de facto sanctioning of corporate cyber retribution is not supported by established legal precedents and norms. Part of the basis for this bias against "offensive cyber" in the law includes the potential for collateral damage on the Internet. An action against a hacker designed to recover a stolen information file or to degrade or damage the computer system of a hacker might degrade or damage the computer or network systems of an innocent third party. The challenges are compounded if the hacker is in one country and the victim in another.

For these reasons and others, the Commission does not recommend specific revised laws under present circumstances. However, current law and law-enforcement procedures simply have not kept pace with the technology of hacking and the speed of the Internet. Almost all the advantages are on the side of the hacker; the current situation is not sustainable. Moreover, as has been shown above, entirely defensive measures are likely to continue to become increasingly expensive and decreasingly effective, while being unlikely to change the cost-benefit calculus of targeted hackers away from attacking corporate networks.

New options need to be considered. As a first step, corporations need better information, and thus an open, two-way communications flow between companies and U.S. government agencies is more necessary than ever before. Companies cannot be asked to share more information unless they have a reasonable expectation that they will receive useful information in return, and they need protections from lawsuits if they do provide information. The Cyber Information Security Protection Act is an example of a statutory effort to address this problem, and the Commission recommends its passage.

Second, an aggressive assessment of the sufficiency of current legal norms to address the new circumstances needs to be undertaken, and new statutes should be considered. The law needs to be clarified to match common sense. The Department of Homeland Security, the Department of Defense, and law enforcement agencies should have the legal authority to use threat-based deterrence systems that operate at network speed against unauthorized intrusions into national security and critical infrastructure networks.

Finally, new laws might be considered for corporations and individuals to protect themselves in an environment where law enforcement is very limited. Statutes should be formulated that protect companies seeking to deter entry into their networks and prevent exploitation of their own network information while properly empowered law-enforcement authorities are mobilized in a timely way against attackers. Informed deliberations over whether corporations and individuals should be legally able to conduct threat-based deterrence operations against network intrusion, without doing undue harm to an attacker or to innocent third parties, ought to be undertaken.

Chapter 14

Potential Future Measures

The Commission considered three additional ideas for protecting the intellectual property of American companies that it does not recommend at this time. In the future, if the loss of IP continues at current levels, these measures ought to be considered.

Recommend that Congress and the administration authorize aggressive cyber actions against cyber IP thieves. Currently, Internet attacks against hackers for purposes of self-defense are as illegal under U.S. law as the attacks by hackers themselves. As discussed in the cyber recommendations above, if counterattacks against hackers were legal, there are many techniques that companies could employ that would cause severe damage to the capability of those conducting IP theft. These attacks would raise the cost to IP thieves of their actions, potentially deterring them from undertaking theses activities in the first place.

The Commission is not ready to endorse this recommendation because of the larger questions of collateral damage caused by computer attacks, the dangers of misuse of legal hacking authorities, and the potential for nondestructive countermeasures such as beaconing, tagging, and self-destructing that are currently in development to stymie hackers without the potential for destructive collateral damage. Further work and research are necessary before moving ahead.

Recommend to Congress and the administration that U.S. funding to the World Health Organization (WHO) program budget in whole or in part be withheld until (1) the WHO's process of certifying national regulatory agencies includes attestation that IP protection is an essential part of the regulatory evaluation process, and (2) the WHO refrains from prequalifying any product until the regulating agency of jurisdiction demonstrates and certifies that it does not violate IP rights. An additional approach—a carrot approach—would be to have a specified WHO contribution by the U.S. government, in addition to current funding, that would be dedicated to developing, implementing, and evaluating the above improvements to the regulatory and prequalification processes.

The U.S. government has leverage at the WHO chiefly because of its financial support, which consists of annual "means tested" contributions to the WHO's program budget and "voluntary" contributions whose total value is about $350 million. This support from the United States can be a carrot or a stick to influence the WHO's actions.

Multilateral coordination may also be possible. For example, the IP of Japanese-developed medicine is frequently stolen, and Japan's current annual and voluntary contributions to the WHO total over $70 million.

The Commission believes this recommendation has strong promise but is not ready to endorse it. To be acted upon, this recommendation requires careful assessment of the likely impacts and the potential for unintended consequences. It will be essential to ensure that the poorest and most vulnerable across the world continue to have access to life-saving, high-quality health interventions, now and in the future. In fact, IP protections are vital to that outcome, because they preserve incentives for innovation and foster predictable markets for manufacturers. Developing consensus around the policy solution among policymakers and manufacturers, particularly regarding the source of any additional funding, will be the necessary next step.

Recommend that Congress and the administration impose a tariff on all Chinese-origin imports, designed to raise 150% of all U.S. losses from Chinese IP theft in the previous year, as estimated by the secretary of commerce. This tariff would be subject to modification by the president on national security grounds.

The argument for this proposal is that only by seriously limiting the U.S. market for Chinese goods and services will sufficient incentive be created for Chinese authorities to systematically reduce IP theft. The method proposed to accomplish that goal is to impose the calibrated tariff just described. While such action would allow retaliation, the huge Chinese trade surplus with the United States could cause the retaliation to be ineffective. Chinese exports to the United States are between three and four times the dollar value of U.S. exports to China.

The Commission is not prepared to make such a recommendation now because of the difficulty of estimating the value of stolen IP, the difficulty of identifying the appropriate imports, and the many legal questions raised by such an action under the United States' WTO obligations. If major IP theft continues or increases, however, the proposal should be further refined and considered.

Dennis C. Blair is the former U.S. Director of National Intelligence. In this role he led sixteen national intelligence agencies, administering a budget of $50 billion and providing integrated intelligence support to the president, Congress, and operations in the field. Prior to rejoining the government, he held the John M. Shalikashvili Chair in National Security Studies with The National Bureau of Asian Research, served as Deputy Director of the Project for National Security Reform, and as a member of the Energy Security Leadership Council of Securing America's Future Energy.

From 2003 to 2006, Admiral Blair was President and Chief Executive Officer of the Institute for Defense Analyses, a federally funded research and development center based in Alexandria, Virginia, that supports the Department of Defense, the Department of Homeland Security, and the intelligence community. He has been a director of two public companies, EDO and Tyco International, and has served on the boards of many nonprofit organizations.

Prior to retiring from the U.S. Navy in 2002, Admiral Blair served as Commander in Chief of U.S. Pacific Command, the largest of the combatant commands. During his 34-year Navy career, he also served on guided missile destroyers in both the Atlantic and Pacific fleets and commanded the Kitty Hawk Battle Group. Ashore, Admiral Blair served as Director of the Joint Staff and held budget and policy positions on the National Security Council and several major Navy staffs.

A graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford University as a Rhodes scholar and was a White House Fellow at the Department of Housing and Urban Development. He has been awarded four Defense Distinguished Service medals and three National Intelligence Distinguished Service medals, and has received decorations from the governments of Japan, Thailand, Korea, Australia, the Philippines, and Taiwan.

Jon M. Huntsman, Jr., is the former U.S. Ambassador to China (2009–11) and former Governor of Utah (2005–9).

Governor Huntsman was appointed U.S. Ambassador to China by President Barack Obama and confirmed by the Senate on August 7, 2009. As ambassador, he focused on working closely with American business owners to facilitate commerce in the growing Asian market and advocating for the release of American citizens wrongfully imprisoned.

As governor, he cut waste and made government more efficient. As a result, Utah held its AAA bond rating and earned national accolades for debt management. Under his leadership, Utah ranked number one in the nation in job creation and was named the best-managed state by the Pew Research Center.

Prior to serving as governor, he was named U.S. Ambassador to Singapore, becoming the youngest head of an American diplomatic mission in a century. Governor Huntsman also served as U.S. Trade Ambassador under President George W. Bush, during which time he helped negotiate dozens of free trade agreements with Asian and African nations.

Governor Huntsman holds a BA in international politics from the University of Pennsylvania.

Craig R. Barrett is a leading advocate for improving education in the United States and around the world. He is also a vocal spokesman for the value technology can provide in raising social and economic standards globally.

Dr. Barrett joined Intel Corporation in 1974 and held positions of Vice President, Senior Vice President, and Executive Vice President from 1984 to 1990. In 1992, he was elected to Intel Corporation's Board of Directors and was promoted to chief operating officer in 1993. Dr. Barrett became Intel's fourth President in 1997, Chief Executive Officer in 1998, and Chairman of the Board in 2005, a post he held until May 2009.

Dr. Barrett has served on numerous boards and policy and government panels. Until June 2009, he was Chairman of the United Nations Global Alliance for Information and Communication Technologies and Development, which works to bring computers and other technology to developing parts of the world. Dr. Barrett has also been an appointee of the President's Advisory Committee for Trade Policy and Negotiations and the American Health Information Community. He has co-chaired the Business Coalition for Student Achievement and the National Innovation Initiative Leadership Council, and has served as a member of the Board of Trustees for the U.S. Council for International Business and the Clinton Global Initiative Education Advisory Board. Dr. Barrett has been a member of the National Governors' Association Task Force on Innovation America, the National Infrastructure Advisory Council, and the Committee on Scientific Communication and National Security, and served on the Board of Directors of the U.S. Semiconductor Industry Association, the National Action Council for Minorities in Engineering, and TechNet.

Dr. Barrett received BS, MS, and PhD degrees in Materials Science from Stanford University. After graduation, he joined the faculty of Stanford University in the Department of Materials Science and Engineering, and remained through 1974. He was a Fulbright Fellow at Danish Technical University in Denmark in 1972 and a NATO Postdoctoral Fellow at the National Physical Laboratory in England from 1964 to 1965.

Slade Gorton is a former U.S. Senator (1981–87 and 1989–2001) and a member of the National Commission on Terrorist Attacks Upon the United States.

Senator Gorton's years in the Senate saw him appointed to powerful committee posts including Appropriations; Budget; Commerce, Science and Transportation; and Energy and Natural Resources. He served as the Chairman of the Interior Appropriations Subcommittee (1995–2001), the Commerce Subcommittees on Consumer Affairs (1995–99), and the Aviation Committee (1999–2000). He was also a member of the Republican leadership as counsel to the majority leader (1996–2000).

Senator Gorton began his political career in 1958 as a Washington State representative, and he went on to serve as state House Majority Leader. In 1968, he was elected Attorney General of Washington State, in which capacity he argued fourteen cases before the U.S. Supreme Court. In June 1980, Senator Gorton received the Wyman Award, the highest honor accorded by the National Association of Attorneys General.

Senator Gorton also served on the President's Consumer Advisory Council (1975–77) and on the Washington State Criminal Justice Training Commission (1969–1981). He was chairman of the Washington State Law & Justice Commission (1969–76), and served as an instructor in constitutional law to public administration graduate students at the University of Puget Sound

Senator Gorton received his BA from Dartmouth College and his JD from Columbia Law School.

William J. Lynn III is the CEO of DRS Technologies, Inc., and former U.S. Deputy Secretary of Defense (2009–2011).

As Deputy Secretary of Defense, Mr. Lynn served under Secretaries Robert Gates and Leon Panetta, managing three million personnel and overseeing an annual budget of $700 billion. He also personally led the department's efforts in cybersecurity, space strategy, and energy policy.

From 2002 to 2009, Mr. Lynn was Senior Vice President of Government Operations and Strategy at the Raytheon Company. Previously, he served as Under Secretary of Defense (Comptroller) from 1997 to 2001 and as Director of Program Analysis and Evaluation in the Office of the Secretary of Defense from 1993 to 1997. Mr. Lynn also worked on the staff of Senator Ted Kennedy as his counsel for the Senate Armed Services Committee.

He has been recognized for numerous professional and service contributions, including four Department of Defense medals for distinguished public service, the Joint Distinguished Civilian Service Award from the Chairman of the Joint Chiefs of Staff, and awards from the U.S. Army, Navy, and Air Force.

Mr. Lynn holds a law degree from Cornell Law School and a master's degree in public affairs from the Woodrow Wilson School of Public and International Affairs at Princeton University. He is also a graduate of Dartmouth College.

Deborah Wince-Smith is the President and CEO of the Council on Competitiveness. Founded in 1986, this unique business-labor-academia coalition of leading CEOs, university presidents, and labor union leaders puts forth actionable public policy solutions to make America more competitive in the global marketplace.

In 2004, Ms. Wince-Smith spearheaded the groundbreaking National Innovation Initiative (NII). The NII shaped the bipartisan America COMPETES Act, created state and regional innovation initiatives, and brought a global focus to innovation. She has also led a bilateral dialogue between the United States and Brazil on competitiveness and innovation strategy, including leading the 2007 and 2010 U.S.-Brazil Innovation Summit.

Ms. Wince-Smith serves as a director of several publicly and privately held companies, leading national and international organizations, and U.S. government advisory committees. She is also a Senate-confirmed member of the Oversight Board of the IRS. She recently chaired the secretary of commerce's Advisory Committee on Strengthening America's Communities and currently serves on the secretary of state's Advisory Committee on International Economic Policy. During her seventeen-year tenure in the federal government, Ms. Wince-Smith held leading positions in the areas of science, technology policy, and international economic affairs. Most notably, she served as the nation's first Senate-confirmed Assistant Secretary of Commerce for Technology Policy in the administration of President George H.W. Bush.

Ms. Wince-Smith received a BA from Vassar College and was one of the first female students to enter King's College at the University of Cambridge, where she read for a master's degree in classical archaeology. In 2006, she received an honorary doctorate in humanities from Michigan State University.

Michael K. Young is the President of the University of Washington. Also a tenured Professor of Law, he has a distinguished record as an academic leader with broad experience in public service and diplomacy. As president of the University of Washington, he leads the nation's top public university (second among all universities) in attracting federal research funding.

Prior to his appointment at the University of Washington, he served as President and Distinguished Professor of Law at the University of Utah. Under President Young's leadership, Utah raised its stature nationally and internationally.

Before assuming the presidency at Utah, he was Dean and Lobingier Professor of Comparative Law and Jurisprudence at the George Washington University Law School. He was also a Professor at Columbia University for more than twenty years, and prior to joining the Columbia University faculty, he served as a law clerk to the late Chief (then Associate) Justice William H. Rehnquist of the U.S. Supreme Court.

President Young has held numerous government positions, including Deputy Under Secretary for Economic and Agricultural Affairs and Ambassador for Trade and Environmental Affairs in the Department of State during the presidency of George H.W. Bush. He also served as a member of the U.S. Commission on International Religious Freedom from 1998 to 2005 and chaired the commission on two occasions.

He has published extensively on a wide range of topics, including the Japanese legal system, dispute resolution, mergers and acquisitions, labor relations, the legal profession, comparative law, industrial policy, international trade law, the North American Free Trade Agreement, the General Agreement on Tariffs and Trade, international environmental law, and international human rights and freedom of religion. He is a member of the Council on Foreign Relations and a Fellow of the American Bar Foundation.

President Young received a BA from Brigham Young University and a JD from Harvard Law School, where he served as a note editor of the *Harvard Law Review*.

LIST OF COMMON ABBREVIATIONS

AmCham China	American Chamber of Commerce in the People's Republic of China
BIO	Biotechnology Industry Organization
BSA	Business Software Alliance
CAFC	Court of Appeals for the Federal Circuit
CBP	U.S. Customs and Border Protection
CFIUS	Committee on Foreign Investment in the United States
EEA	Economic Espionage Act of 1996
FBI	Federal Bureau of Investigation
FDI	Foreign Direct Investment
FTC	U.S. Federal Trade Commission
GDP	Gross Domestic Product
GIPA	Global Intellectual Property Academy
IDC	International Data Corporation
IP	intellectual property
IPEC	Intellectual Property Enforcement Coordinator
IPR	intellectual property rights
OECD	Organisation for Economic Co-operation and Development
PLA	People's Liberation Army
PRC	People's Republic of China
SEC	U.S. Securities and Exchange Commission
SOE	state-owned enterprise
STEM	science, technology, engineering, and mathematics
TRIPS	Trade-Related Aspects of Intellectual Property Rights
USGAO	U.S. Government Accountability Office
USITC	U.S. International Trade Commission
USPTO	U.S. Patent and Trademark Office
USTR	U.S. Trade Representative
VOG	volume of goods
WIPO	World Intellectual Property Organization
WHO	World Health Organization
WTO	World Trade Organization

THE IP COMMISSION

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY

The Commission on the Theft of American Intellectual Property is an independent and bipartisan initiative of leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics. The three purposes of the Commission are to:

1. Document and assess the causes, scale, and other major dimensions of international intellectual property theft as they affect the United States
2. Document and assess the role of China in international intellectual property theft
3. Propose appropriate U.S. policy responses that would mitigate ongoing and future damage and obtain greater enforcement of intellectual property rights by China and other infringers

COMMISSIONERS:

Dennis C. Blair
Co-chair

Jon M. Huntsman, Jr.
Co-chair

Craig R. Barrett

William J. Lynn III

Slade Gorton

Deborah Wince-Smith

Michael K. Young