2015

Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats

Peter K. Yu
Drake University Law School

TRADE SECRET HACKING, ONLINE DATA BREACHES, AND CHINA'S CYBERTHREATS

Peter K. Yu†

TABLE OF CONTENTS

INTRODUCTION

Online hacking from China, Iran, North Korea, Russia, and other parts of the world has caught the attention of U.S. policymakers, commentators, and the American public. For example, the discussion of the systematic attacks launched by potentially government-sponsored Chinese hackers reinforces the view that China is using all means necessary to compete against the United States.[1] After years of cyberattacks linked to Unit 61398 of the People's Liberation Army, which is also known as the "Comment Crew" or the "Shanghai Group," the U.S. Department of Justice finally issued a symbolic indictment of

 Kern Family Chair in Intellectual Property Law and Director, Intellectual Property Law Center, Drake University Law School. An earlier version of this Article was presented at the "Protecting Trade Secrets in Asia and the United States" Conference at John Marshall Law School in Chicago. The Author is grateful to Doris Long for her hospitality, and Derek Bambauer and the conference participants for their valuable comments and suggestions.

[1] For discussions of China's cyberthreat, see generally CHINA AND CYBERSECURITY: ESPIONAGE, STRATEGY, AND POLITICS IN THE DIGITAL DOMAIN (Jon R. Lindsay et al., 2015) [hereinafter CHINA AND CYBERSECURITY]; DENNIS F. POINDEXTER, THE CHINESE INFORMATION WAR: ESPIONAGE, CYBERWAR, COMMUNICATIONS CONTROL AND RELATED THREATS TO UNITED STATES INTERESTS (2013); CARL ROPER, TRADE SECRET THEFT, INDUSTRIAL ESPIONAGE, AND THE CHINA THREAT (2014).

its five group members.[2] Research published by the Information Warfare Monitor, including a rather disturbing report on GhostNet, also traced cyberespionage and other intrusive activities back to computers located in China.[3]

Most recently, the unprecedented cyberattack on Sony's movie studio—allegedly from North Korea[4]—delayed and scaled back the nationwide theatrical release of the film *The Interview*.[5] The intrusion not only embarrassed studio executives and Hollywood in general, but also raised cybersecurity concerns among the U.S. business community.[6] In the wake of this attack, President Barack Obama called for greater cooperation between the government and the private sector to protect cybersecurity and the country's critical infrastructure,[7] which includes "oil pipelines, railroad tracks, water treatment facilities and the power grid."[8] He also issued an executive order to promote the voluntary "sharing of information related to cybersecurity risks and incidents."[9]

Taking advantage of the forum provided by this timely Symposium, this Article closely examines the ongoing debate on China's sustained effort in using online hacking and other intrusive techniques to steal trade secrets and proprietary data from U.S.

---

2 *See* Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES, May 20, 2014, at A1 (reporting the indictment).

3 INFO. WARFARE MONITOR, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK (2009); INFO. WARFARE MONITOR & SHADOWSERVER FOUND., SHADOWS IN THE CLOUD: INVESTIGATING CYBER ESPIONAGE 2.0 (2010); *see also* Sarah McKune, *"Foreign Hostile Forces": The Human Rights Dimension of China's Cyber Campaigns*, *in* CHINA AND CYBERSECURITY, *supra* note 1, at 260, 274 ("While these investigations did not generate conclusive evidence of Chinese government backing, the interest and/or involvement of the Chinese state is probable in light of the targeted entities and technical forensics indicating China as the location of the command-and-control servers employed.").

4 *But see* Nicole Perlroth, *Experts Question U.S. Account of Sony Hacking*, N.Y. TIMES, Dec. 29, 2014, at B4 (stating that "private security researchers are increasingly voicing doubts that the hack of Sony's computer systems was the work of North Korea").

5 *See* David E. Sanger & Nicole Perlroth, *U.S. Is Said to Find North Korea Behind Cyberattack on Sony*, N.Y. TIMES, Dec. 18, 2014, at A1 (reporting that "the four largest theater chains in the United States—Regal Entertainment, AMC Entertainment, Cinemark and Carmike Cinemas—and several smaller chains said they would not show 'The Interview' as a result of the [terrorist] threat").

6 *See* Michael Cieply & Brooks Barnes, *Sony Attack Is Unraveling Relationships in Hollywood*, N.Y. TIMES, Dec. 19, 2014, at B1 (reporting that "[t]he attack has disrupted the web of executive, business and talent relationships that stitches together Sony's core moviemaking operation"); Michael Cieply & Brooks Barnes, *Sony's Dirty Laundry, for All to See*, N.Y. TIMES, Dec. 11, 2014, at B1 (reporting the disclosure of executive salaries, unpublished scripts, sensitive contracts, aliases used by stars to check into hotels, and a highly embarrassing email exchange between Sony's co-chairwoman and a film producer).

7 Nicole Perlroth & David E. Sanger, *Obama Calls for New Cooperation to Wrangle the "Wild West" Internet*, N.Y. TIMES, Feb. 14, 2015, at B1.

8 Nicole Perlroth, *Hacked vs. Hackers: Game On*, N.Y. TIMES, Dec. 3, 2014, at F1.

9 Exec. Order No. 13,691 (Feb. 13, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

businesses. Part I outlines the five common narratives that have thus far been advanced to recount this widely criticized effort. Sensing the narratives' negative overtones, Part II offers five modest suggestions on how a more positive debate can be constructed to help identify ways to reduce online hacking and data breaches as well as to enhance the protection of trade secrets and proprietary data.

I. FIVE COMMON NARRATIVES

From ancient Egyptians to the Warring States in China, espionage and intelligence activities have been undertaken for millennia to collect information and to steal military secrets.[10] While these activities received wide news coverage during the Cold War era, many of them have now migrated to the digital environment, the Internet in particular. Owing to "its logistical advantages and the promise of plausible deniability," the online environment is especially attractive.[11] Indeed, the recent proliferation of online hacking and data breaches from abroad have led policymakers and commentators to discuss these activities in connection with cyberwarfare, information warfare, or what Eric Schmidt and Jared Cohen recently popularized as the "New Code War."[12]

Nevertheless, what China has been accused of seems to be quite different from what the Soviet Union used to do during the Cold War era. Instead of stealing state and military secrets, Chinese hackers are now also targeting business, technical, scientific, and industrial information.[13] It is therefore understandable why Chinese hacking activities have become a major concern for U.S. policymakers and businesses alike.

To the Obama administration, for example, "there is a major

---

[10] *See* RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 230 (2010) ("Nations have been engaging in espionage at least since biblical times."); Nigel Inkster, *The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace*, *in* CHINA AND CYBERSECURITY, *supra* note 1, at 29, 29 ("The concept of intelligence is . . . well entrenched in Chinese culture dating back to the time of the warring states (c. 475–221 B.C.), when Sunzi's *Art of War* (*Sunzi bingfa*), which deals at length with the subject of espionage, appeared.").

[11] WILLIAM C. HANNAS ET AL., CHINESE INDUSTRIAL ESPIONAGE: TECHNOLOGY ACQUISITION AND MILITARY MODERNISATION 218 (2013); *see also* INFO. WARFARE MONITOR, *supra* note 3, at 12 ("[T]he challenge of identifying perpetrators and understanding their motives gives state actors convenient *plausible deniability* and the ability to officially distance themselves from attacks."); ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 104 (2013) ("A cyber attack might be the state's perfect weapon: powerful, customizable and anonymous.").

[12] SCHMIDT & COHEN, *supra* note 11, at 112.

[13] *See* ROPER, *supra* note 1, at xiii ("When the USSR was still in existence, information collected was more of military and political in nature. Since its demise, more theft has occurred, with China being the culprit this time—in both volume and specificity—and it is not just military or political, but runs the entire gamut of just about every area you could think of.").

difference between spying for national security purposes, something the United States does daily, and the commercial, for-profit espionage carried out by China's military."[14] As reported in *The New York Times*:

> [W]hen Mr. Obama raised the issue [about online hacking] with Xi Jinping, the Chinese president, he focused only on commercial espionage, arguing it is far more pernicious to use the intelligence instruments of the state for a business advantage. The United States may do all it can to learn about China's nuclear arsenal, or Beijing's intentions in its territorial disputes with Japan, but it does not, he says, steal from China Telecom to help AT&T.[15]

The line the U.S. administration draws between fair play and foul play, however, is not as clear as one would expect. Not only do most countries—democratic or otherwise—fail to recognize it,[16] this line is also not always drawn in situations involving U.S. intelligence and surveillance efforts. As *The New York Times* continued in its report:

> [T]he United States spies regularly for economic advantage when the goal is to support trade talks; when the Clinton administration was locked in a high-stakes negotiation in the 1990s to reach an accord with Japan, it bugged the Japanese negotiator's limousine. At the time, the chief beneficiaries would have been the Big Three auto companies and a smattering of parts suppliers. It is also widely believed to be using intelligence in support of trade negotiations underway with European and Asian trading partners.[17]

In addition, a top secret document obtained by Edward Snowden, a former National Security Agency contractor, showed that "an American law firm [had been] monitored while representing a foreign government in trade disputes with the United States," the lawyers' attorney-client privilege notwithstanding.[18] If the U.S. administration considered it a matter of national security to spy on a local law firm defending a foreign government in a trade dispute, it is not difficult to understand why other countries have had a tough time drawing the line between commercial espionage and national security. This difficulty is particularly acute in a country such as China, given the perceived

---

14 David E. Sanger, *With Spy Charges, U.S. Draws a Line That Few Others Recognize*, N.Y. TIMES, May 20, 2014, at A8.

15 *Id.*

16 *See id.* ("[W]hile American officials are loath to admit it, Washington's view has relatively few advocates around the world. The French, for example, were notorious for conducting state-backed corporate espionage long before the Chinese mastered the form."); Jon R. Lindsay, *Introduction: China and Cybersecurity: Controversy and Context*, *in* CHINA AND CYBERSECURITY, *supra* note 1, at 1, 13 ("American attempts to articulate the difference between the political-military targets of US cyber espionage and the economic targets of Chinese espionage, or between Internet control as practiced by China and metadata collection as practiced by the [National Security Agency], have tended to fall on deaf ears.").

17 Sanger, *supra* note 14.

18 James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 16, 2014, at A1.

"overlap between security and economic concerns" among Chinese policymakers[19] and the continued domination of state-owned enterprises in the local business environment. It is also worth recalling that the Obama administration has repeatedly invoked national security to justify the nondisclosure of the negotiating texts of the Anti-Counterfeiting Trade Agreement and the Trans-Pacific Partnership Agreement.[20]

Thus far, five common narratives have emerged concerning the online hacking and data breaches conducted by Chinese hackers. This Article will examine each narrative in turn.

A. *U.S. Businesses*

The first narrative focuses on the interests and frustrations of U.S. businesses. The lack of protection and enforcement of intellectual property rights in China has been the subject of a perennial debate about China.[21] Although the country's accession to the World Trade Organization (WTO), repeated amendments of intellectual property laws and regulations, and increased provision of enforcement resources have greatly strengthened the protection and enforcement of intellectual property rights, the protection of trade secrets and proprietary data remains inadequate—and, from the standpoint of U.S. rights holders, woefully inadequate.

In March 2014, for instance, a former DuPont employee and his accomplice were found guilty of selling to a Chinese company DuPont's trade secret concerning the use of titanium dioxide to whiten products.[22] This conviction joined a long line of convictions and arrests

---

[19] Adam Segal, *Chinese Economic Statecraft and the Political Economy of Asian Security*, *in* CHINA'S RISE AND THE BALANCE OF INFLUENCE IN ASIA 146, 147 (William W. Keller & Thomas G. Rawski eds., 2007); *see also* Schmidt & Sanger, *supra* note 2 (noting that "the Chinese, with their vast state-owned enterprises, many run by the People's Liberation Army, have often argued that economic security and national security are one").

[20] For discussions of a lack of transparency in the negotiations surrounding these agreements, see generally David S. Levine, *Bring in the Nerds: Secrecy, National Security, and the Creation of International Intellectual Property Law*, 30 CARDOZO ARTS & ENT. L.J. 105 (2012); Peter K. Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. REV. 975, 998–1019 (2011).

[21] For the Author's earlier discussions on piracy and counterfeiting in China, see generally Peter K. Yu, *Intellectual Property, Economic Development, and the China Puzzle*, *in* INTELLECTUAL PROPERTY, TRADE AND DEVELOPMENT: STRATEGIES TO OPTIMIZE ECONOMIC DEVELOPMENT IN A TRIPS-PLUS ERA 173 (Daniel J. Gervais ed., 1st ed. 2007) [hereinafter Yu, *China Puzzle*]; Peter K. Yu, *From Pirates to Partners: Protecting Intellectual Property in China in the Twenty-First Century*, 50 AM. U. L. REV. 131 (2000); Peter K. Yu, *From Pirates to Partners (Episode II): Protecting Intellectual Property in Post-WTO China*, 55 AM. U. L. REV. 901 (2006); Peter K. Yu, *The Middle Kingdom and the Intellectual Property World*, 13 OR. REV. INT'L L. 209 (2011).

[22] Karen Gullo, *California Man Guilty of Stealing DuPont Trade Secrets*, BLOOMBERGBUSINESS (Mar. 5, 2014, 5:29 PM), http://www.bloomberg.com/news/2014-03-05/california-man-guilty-of-stealing-dupont-trade-secrets.html.

generated from Chinese industrial espionage activities.[23] Following the DuPont case and other similar complaints, the United States Trade Representative (USTR) raised the priority of trade secret protection in the China enforcement agenda. As he stated in the *2014 Special 301 Report*:

> [T]rade secret theft is a serious and growing problem in China. Thefts may arise in a variety of circumstances, including those involving departing employees, failed joint ventures, and cyber intrusion and hacking. In addition, thefts arising from the misuse of information submitted to government entities for purposes of complying with regulatory obligations are particularly troubling. The misappropriation of trade secrets and their use by a competing enterprise can have a devastating impact on a company's business, making recourse to adequate and effective legal remedies particularly important.[24]

According to this report, cyberintrusion and online hacking have been repeatedly used to steal trade secrets and proprietary data from U.S. businesses. Also of concern are the "thefts arising from the misuse of information submitted to government entities for purposes of complying with regulatory obligations."[25] Such information includes the undisclosed clinical trial data submitted by U.S. pharmaceutical and agrochemical industries to Chinese regulatory authorities.[26]

China's need for trade secrets, proprietary data, and other confidential information is understandable considering its ongoing and rapidly growing efforts to boost independent innovation. These efforts were driven in large part by such government policies as the Outline of the National Medium- and Long-Term Plan for Science and Technology Development (2006–2020) and the Outline of the National Intellectual Property Strategy.[27] These outlines were released by the State Council

---

[23] *See* HANNAS ET AL., *supra* note 11, at 256–70 (providing the case histories of Chinese industrial espionage).

[24] OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE [USTR], 2014 SPECIAL 301 REPORT 32 (2014) [hereinafter 2014 SPECIAL 301 REPORT].

[25] *Id.*

[26] For discussions of the protection of clinical trial data, see generally Carlos M. Correa, *Protecting Test Data for Pharmaceutical and Agrochemical Products Under Free Trade Agreements*, *in* NEGOTIATING HEALTH: INTELLECTUAL PROPERTY AND ACCESS TO MEDICINES 81 (Pedro Roffe et al. eds., 2006) [hereinafter NEGOTIATING HEALTH]; Meir Perez Pugatch, *Intellectual Property, Data Exclusivity, Innovation and Market Access*, *in* NEGOTIATING HEALTH, *supra*, at 97; Jerome H. Reichman, *The International Legal Status of Undisclosed Clinical Trial Data: From Private to Public Goods?*, *in* NEGOTIATING HEALTH, *supra*, at 133; Robert Weissman, *Data Protection: Options for Implementation*, in NEGOTIATING HEALTH, *supra*, at 151; Aaron Xavier Fellmeth, *Secrecy, Monopoly, and Access to Pharmaceuticals in International Trade Law: Protection of Marketing Approval Data Under the TRIPs Agreement*, 45 HARV. INT'L L.J. 443 (2004).

[27] *See* Peter K. Yu, *Five Oft-repeated Questions About China's Recent Rise as a Patent Power*, 2013 CARDOZO L. REV. DE NOVO 78, 88–96 (discussing these outlines and China's independent innovation policies).

in February 2006 and June 2008, respectively.

B. *Chinese Businesses*

The second narrative concerns the interests of Chinese businesses. Although these businesses do not always appreciate the external pressure the USTR has exerted on their government, they see the benefits of legal reforms and improvements in the intellectual property regime. Like their foreign counterparts, Chinese businesses are deeply frustrated by the inadequate protection local laws have afforded to trade secrets, proprietary data, and other confidential information. The lack of intellectual property protection may also have cost them more than their foreign counterparts.[28]

To be fair, China already offers trade secret protection under its contract, criminal, intellectual property, joint venture, labor, and tort laws.[29] Nevertheless, because the protection comes from many different statutes and regulations, it is piecemeal at best. Even worse, the Law Against Unfair Competition—the statute of choice for many rights holders—is badly outdated. This statute was enacted the year after China and the United States signed the 1992 Memorandum of Understanding on the Protection of Intellectual Property[30] and close to a decade before China joined the WTO.[31] Since its enactment in 1993, this unfair competition law has not been revised, even though consultations about its revision have already begun.[32] The lack of legislative overhaul in this area stands in sharp contrast to the repeated amendment of other intellectual property laws. While the Patent and Trademark Laws have already been amended three times, the Copyright Law is now undergoing its third wholesale revision.[33]

---

[28] *See* Barry Naughton & Yao Yang, *The Economic Relationship*, *in* DEBATING CHINA: THE U.S.–CHINA RELATIONSHIP IN TEN CONVERSATIONS 21, 29 (Nina Hachigian ed., 2014) ("[W]eak [intellectual property] protection not only hurts American firms but Chinese firms as well. In fact, it may hurt Chinese firms more.").

[29] *See* SHAN HAILING, THE PROTECTION OF TRADE SECRETS IN CHINA 35–37 (2008); Liu Xiaohai, *Unfair Competition/Trade Secrets/Know-how (2)*, *in* CHINESE INTELLECTUAL PROPERTY AND TECHNOLOGY LAWS 127, 136–38 (Rohan Kariyawasam ed., 2011) [hereinafter CHINESE IP LAWS].

[30] Memorandum of Understanding on the Protection of Intellectual Property, Jan. 17, 1992, China–U.S., T.I.A.S. No. 12036 (1995). Although an earlier memorandum of understanding covering software protection was signed in 1989, the 1992 memorandum was the "first full bilateral [intellectual property] agreement" between China and the United States. Joseph A. Massey, *The Emperor Is Far Away: China's Enforcement of Intellectual Property Rights Protection, 1986–2006*, 7 CHI. J. INT'L L. 231, 235 (2006).

[31] China formally became the 143rd WTO member on December 11, 2001. *Members and Observers*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited Apr. 5, 2015).

[32] *See* Liu, *supra* note 29, at 160.

[33] The Third Amendment to the Patent Law was adopted in December 2008, while the Third Amendment to the Trademark Law was adopted in August 2013. For a discussion of the

To local businesses, the external push by the USTR and American businesses for trade secret reform can therefore be beneficial even if they dislike foreign criticisms. Such a push would help generate the momentum needed for legal reform. It would also enable local businesses to preserve the hard-earned political capital for future actions. In fact, external pressure has historically played a critical role in fostering intellectual property reforms in China. Leading examples are the establishment of the modern intellectual property system in the 1980s and the strengthening of intellectual property rights in the run-up to China's WTO accession.[34]

Notwithstanding the eagerness of local businesses to join their foreign counterparts in pushing for trade secret reform, it remains unclear whether the Law Against Unfair Competition will be merely updated or whether a new trade secret law will be introduced.[35] While an updated statute would certainly provide rights holders—local and foreign alike—with stronger protection, the latter seems to be what U.S. businesses prefer. After all, the current unfair competition law was written from a focus on unfair competition and anti-monopoly protection.[36] The statute does not protect trade secrets as a form of property the same way U.S. trade secret laws do.[37]

---

evolution of the Chinese patent system, see generally Peter K. Yu, *Building the Ladder: Three Decades of Development of the Chinese Patent System*, 5 WIPO J. 1 (2013) [hereinafter Yu, *Building the Ladder*].

[34] *See* Yu, *China Puzzle*, *supra* note 21, at 185–88 (discussing how the external pressure exerted by the United States provided the momentum needed for the early intellectual property reforms in China).

[35] *See* Liu, *supra* note 29, at 161 ("Scholars and practitioners . . . suggest establishing a special law for the protection of trade secrets; however, no such official legislative plan exists at present.").

[36] For discussions of Chinese trade secret laws, see generally SHAN, *supra* note 29; Hu Kaizhong, *Unfair Competition/Trade Secrets (1)*, *in* CHINESE IP LAWS, *supra* note 29, at 106; Liu, *supra* note 29.

[37] *Compare* Sharon K. Sandeen, *The Limits of Trade Secret Law: Article 39 of the TRIPS Agreement and the Uniform Trade Secrets Act on Which It Is Based*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 537, 546–47 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) [hereinafter TRADE SECRECY HANDBOOK] ("By some accounts, the United States insisted [during the TRIPS negotiations] that trade secrets were a form of property and resisted tying trade secret protection to unfair competition principles."), *with* Fan Buzhengdang Jingzheng Fa [Law of the People's Republic of China Against Unfair Competition] art. 1 (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 2, 1993, effective Dec. 1, 1993), *available at* http://www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383803.htm ("This Law is formulated with a view to safeguarding the healthy development of socialist market economy, encouraging and protecting fair competition, repressing unfair competition acts, and protecting the lawful rights and interests of business operators and consumers."); Hu, *supra* note 36, at 109 (stating that the Law Against Unfair Competition "attempts to reflect current business practice in commercial markets and the need to regulate market competition").

C. *Chinese Government Officials*

The third narrative draws on the positions taken by Chinese government officials, especially those hardliners who frequently condemn the external pressure exerted by the USTR and American businesses. Indeed, past pressures and accusations from the United States have led to kneejerk protests and oppositions from Chinese officials. As Chinese Foreign Minister Ma Zhaoxu declared: "We urge the US to abandon its Cold War mindset, stop making groundless accusations against China, and do more to improve mutual trust between the two nations and friendship between the two peoples."[38]

The reactions of these officials are unsurprising, considering that online hacking and information warfare have been practiced by virtually all countries capable of such practices,[39] the United States included.[40] In their recent book, *Cyber War*, Richard Clarke, the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, and Robert Knake observed:

> U.S. intelligence officials do not . . . rate China as the biggest threat

---

[38] *Espionage Accusations Against China "Groundless,"* CHINA.ORG.CN (May 15, 2009), http://china.org.cn/international/2009-05/15/content_17780594.htm.

[39] As Major Arie Schaap of the U.S. Air Force observed:

> As of 2007, there were an estimated 120 countries working on cyber attack commands, and in 10 to 20 years experts believe we could see countries jostling for cyber supremacy. States are no doubt preparing to launch international all-out online attacks and the current political environment includes countries testing the waters to gauge the potential influence, and risks, of such assaults. The assistant director of the FBI's cyber division stated that computer attacks pose the biggest risk "from a national security perspective, other than a weapon of mass destruction or a bomb on one of our major cities." NATO's Chief of Cyber Defense concurs, stating that "cyber terrorism [and] cyber attacks pose as great a threat to national security as a missile attack."

Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121 (2009) (footnotes omitted); *see also* ROPER, *supra* note 1, at xiii ("China is not alone in collecting information for its own economic and military expansion. To some extent, every country seeks out information on other countries."); POINDEXTER, *supra* note 1, at 121–22 ("Real spying . . . is done by almost every government in the world. If the Chinese spy on us, they do it with clear understanding that we spy on them too. Every country spies on the others as much as they can support. In all the world's governments we understand spying and expect it.").

[40] A notable example is the computer worm Stuxnet, which Israel and the United States jointly designed to infiltrate the computers controlling Iran's nuclear enrichment program. Derek Bambauer called this worm "the most advanced cyberweapon built to date." Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1015 (2014). As he recounted:

> [Stuxnet] performed two clever tasks: it sped up the centrifuges that enrich uranium, damaging some irreparably, and it concealed the acceleration from the engineers monitoring the system. Stuxnet recorded data from normal centrifuge operations and, while sabotaging the centrifuges, replayed the normal data to the engineers, falsely reassuring them. One piece of sophisticated malware succeeded where diplomacy and threats of military force failed—it set back Iran's attempts to craft a nuclear weapon by at least a year, and likely longer.

Id. (footnotes omitted).

> to the U.S. in cyberspace. "The Russians are definitely better, almost as good as we are," said one. There seems to be a consensus that China gets more attention because, intentionally or otherwise, it has often left a trail of bread crumbs that can be followed back to Tiananmen Square. . . . Other nations known to have skilled cyber war units are Israel and France. U.S. intelligence officials have suggested that there are twenty to thirty militaries with respectable cyber war capability, including those of Taiwan, Iran, Australia, South Korea, India, Pakistan, and several NATO states. "The vast majority of the industrialized countries in the world today have cyber-attack capabilities," said former Director of National Intelligence Admiral Mike McConnell.[41]

Even more troubling for Chinese officials, the United States's accusations often ignore the significant progress China has made in the intellectual property arena as well as the considerable resources that the country has poured into intellectual property enforcement in the past decade. To date, China not only has built a new intellectual property system from the ground up faster than any other country in history,[42] it also has the world's largest volume of intellectual property litigation.[43] At some point, one has to query whether the scale of piracy and counterfeiting in China has been so enormous that the expectations of the USTR and American businesses are somewhat unrealistic.

For many Chinese officials, the United States's accusations are also highly disturbing, as they fail to take note of China's recent re-emergence as an innovative power.[44] Since 2012, more than two million patent applications have been filed annually with the State Intellectual Property Office.[45] This two million figure was a target for 2015 in

---

41 CLARKE & KNAKE, *supra* note 10, at 63–64.

42 *See* Yu, *Building the Ladder*, *supra* note 33, at 15; *see also* Jack Valenti, Letter to the Editor, *China's Pirated Disks*, N.Y. TIMES, Apr. 3, 1998, at A26 ("China has accomplished what no other country has achieved.").

43 *See* J. Benjamin Bai & Da Guoping, *Strategies for Trade Secrets Protection in China*, 9 NW. J. TECH. & INTELL. PROP. 351, 351 (2011) ("China became the world's most litigious country for intellectual property disputes in 2005, surpassing the U.S. in the number of intellectual property lawsuits filed annually."); Xuan-Thao Nguyen, *The China We Hardly Know: Revealing the New China's Intellectual Property Regime*, 55 ST. LOUIS L.J. 773, 775 (2011) ("In 2005, there were 12,159 patent, copyright, and trademark cases filed in the United States, compared to 10,825 cases in China. In 2006, the United States saw 11,486 cases, while China witnessed 11,436 intellectual property cases. The trend continues, as demonstrated by the fact that the number of intellectual property cases filed in 2007 for the United States totaled 10,761, whereas China's was 15,159."); Peter K. Yu, *The Rise and Decline of the Intellectual Property Powers*, 34 CAMPBELL L. REV. 525, 544–49 (2012) [hereinafter Yu, *Rise and Decline*] (discussing the potential intellectual property litigation explosion in China).

44 For discussions of China's rise as an innovative power, see generally SHAUN REIN, THE END OF COPYCAT CHINA: THE RISE OF CREATIVITY, INNOVATION, AND INDIVIDUALISM IN ASIA (2014); Yu, *Rise and Decline*, *supra* note 43, at 529–32; Richard P. Suttmeier & Yao Xiangkui, *China's IP Transition: Rethinking Intellectual Property Rights in a Rising China* (The National Bureau of Asian Research, NBR Special Report No. 29, 2011), *available at* http://china-us.uoregon.edu/pdf/IP_report.pdf.

45 *Comparative Table 1 Contemporary Quantity Comparison of Three Kinds of Patents*

China's National Patent Development Strategy.[46] Although David Kappos, the then-director of the U.S. Patent and Trademark Office, found the announced target "mind-blowing,"[47] that figure was already surpassed three years ago.

In addition, according to the statistics from the World Intellectual Property Organization, China had the world's third largest volume of applications under the Patent Cooperation Treaty (PCT) in 2014, behind only the United States and Japan.[48] Among all the corporate applicants, Huawei Technologies and ZTE Corporation had the largest and third largest number of PCT applications, respectively.[49] In the same period, China also ranked seventh in filing international trademark applications under the Madrid Agreement Concerning the International Registration of Marks and its related protocol.[50] With 20,309 designations, China was the world's "most designated member country in international registrations" within the Madrid System.[51]

Given the progress China has made in the trademark and patent areas—and, to some extent, also the copyright area[52]—one cannot help but wonder whether the USTR and American businesses are simply going down the list of intellectual property demands. These demands started off with copyrights, patents, and trademarks—issues that were highly contentious in the 1980s and 1990s. Now that these demands have been largely met, the *demandeurs* seem to have just moved on to trade secrets and other areas of intellectual property law.

Although it is logical for *demandeurs* to go down their list of demands, this approach is particularly frustrating and demoralizing to Chinese policymakers, as it suggests the impossibility of satisfying the USTR and American businesses. In the view of these policymakers, China will be accused of intellectual property theft regardless of the progress it has made in the intellectual property field. Even worse, the *demandeurs* seem to have a rather narrow focus—a focus that is driven not by an overall analysis, but by the U.S. competitive advantage. Thus, from the standpoint of many Chinese policymakers, unless China focuses its reform on rights that benefit U.S. rights holders, the progress the country has made in other areas of intellectual property law will be

---

Received from Home and Domestic Between 2011 and 2012, STATE INTELL. PROP. OFF. P.R.C. (Jan. 22, 2013), http://english.sipo.gov.cn/statistics/2012/12/201303/t20130315_788163.html.

46 Steve Lohr, *When Innovation, Too, Is Made in China*, N.Y. TIMES, Jan. 2, 2011, at BU3 (quoting David Kappos, Director, U.S. Patent and Trademark Office).

47 *Id.*

48 Press Release, World Intellectual Property Org., Telecoms Firms Lead WIPO International Patent Filings, World Intellectual Property Org. Press Release PR/2015/774 (Mar. 19, 2015), *available at* http://www.wipo.int/pressroom/en/articles/2015/article_0004.html.

49 *Id.*

50 *Id.*

51 *Id.*

52 *See* Yu, *Rise and Decline*, *supra* note 43, at 576–77 (suggesting that the improvements in the copyright area may not be as dramatic as those in the patent area).

conveniently ignored.

More damningly for the United States, just as the Obama administration was heavily criticizing China for hacking into computers on U.S. soil, news about Edward Snowden and the U.S. government's global surveillance program received front-page coverage.[53] This coverage not only caused the United States to lose its moral high ground, but also provided a vivid reminder that all governments conduct surveillance and intelligence activities. To a large extent, the news about Snowden was as ill-timed as Secretary Tommy Thompson's reported threat to break Bayer's patent on ciprofloxacin following the anthrax attacks in 2001.[54] Most policymakers and commentators from abroad considered his threat hypocritical because around that time the USTR and the American pharmaceutical industry were aggressively pressuring South Africa and other developing countries to stop issuing compulsory licenses to address public health crises, including those brought about by HIV/AIDS, tuberculosis, and malaria.[55]

Moreover, many U.S. allies, such as France, have actively practiced industrial espionage. As reported on CBS News, leaked U.S. diplomatic cables showed that "France [had been] the country that conduct[ed] the most industrial espionage on other European countries, even ahead of China and Russia."[56] An editorial from *The New York Times* also noted France's "aggressi[on] in spying to benefit domestic companies."[57] If the U.S. administration is willing to look the other way in the case of France, why does it single out China for its complaints? Did the charges suggest a double standard? Or did they represent yet

---

53 As a local expert quoted in *China Daily* declared: "For months, Washington has been accusing China of cyberespionage, but it turns out the biggest threat to the pursuit of individual freedom and privacy in the U.S. is the unbridled power of the government." Joe Nocera, *This Isn't How to Stop Hacking*, N.Y. TIMES, June 15, 2013, at A21.

54 *See* Debora Halbert, *Moralized Discourses: South Africa's Intellectual Property Fight for Access to AIDS Drugs*, 1 SEATTLE J. SOC. JUST. 257, 280 (2002) (discussing the anthrax attacks in the United States).

55 *See id.* ("The U.S. lost significant international legitimacy when the overwhelming hypocrisy of its own efforts regarding anthrax were juxtaposed against the efforts of developing countries to secure cheap access to AIDS drugs."); José Marcos Nogueira Viana, *Intellectual Property Rights, the World Trade Organization and Public Health: The Brazilian Perspective*, 17 CONN. J. INT'L L. 311, 313 (2002) ("U.S. and Canadian approaches to the anthrax scare is precisely what the Brazilian government has been doing over the past two years in response to HIV/AIDS."); Peter K. Yu, *TRIPS Enforcement and Developing Countries*, 26 AM. U. INT'L L. REV. 727, 777–78 (2011) (noting that "the United States' short-sighted exploration of compulsory licensing as an option to lower the price of ciprofloxacin following anthrax attacks in 2001 . . . suggested a double standard").

56 Joshua Norman, *WikiLeaks: France Leads Russia, China in Industrial Spying in Europe*, CBS NEWS (Jan. 4, 2011, 11:02 AM), http://www.cbsnews.com/news/wikileaks-france-leads-russia-china-in-industrial-spying-in-europe.

57 Editorial, *America, China and the Hacking Threat*, N.Y. TIMES, May 25, 2014, at SR10; *see also* David E. Sanger & Tim Weiner, *Emerging Role for the C.I.A.: Economic Spy*, N.Y. TIMES, Oct. 15, 1995, § 1, at 1 ("France has spied on American companies for years, planting moles in companies like Boeing and Texas Instruments and breaking into hotel rooms to rifle through attache cases.").

another round of complaints that the administration had to mount to diffuse domestic political pressure?

D. *TRIPS Commentators*

The fourth narrative pertains to the commentary on the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). Article 39.2 of the Agreement specifically protects information that "is secret . . . [,] has commercial value . . . and . . . has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[58] Although the protection offered in this provision is modelled after the Uniform Trade Secrets Act in the United States,[59] the language eventually adopted in the TRIPS Agreement remains broad and vague.

Equally problematic is Article 39.3 of the TRIPS Agreement, which mandates protection against the unfair commercial use of clinical trial data that have been submitted to regulatory agencies for the approval of pharmaceutical or agrochemical products that have utilized new chemical entities.[60] While the bilateral, regional, and plurilateral trade agreements that the United States established in the past decade called for the institution of a data exclusivity regime,[61] Article 39.3 does not introduce such a requirement.

More disappointing to the U.S. pharmaceutical and agrochemical industries, the TRIPS language includes four additional limitations. First, Article 39.3 protects pharmaceutical or agrochemical products that have "utilize[d] new chemical entities."[62] It does not intend to cover "existing chemical entities that have been reformulated or sold for a new indication."[63] Second, Article 39.3 protects regulatory data "against unfair commercial use."[64] With a specific purpose in mind, the provision does not offer general protection to, or create exclusive rights

---

58 Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39.2, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 (1994) [hereinafter TRIPS Agreement].

59 *See* Sandeen, *supra* note 37, at 538 ("Subsections (a) through (c) of Article 39(2) are modeled after the definition of 'trade secret' that is contained in the Uniform Trade Secrets Act . . . and are used to define the type and scope of information that must be protected.").

60 TRIPS Agreement art. 39.3.

61 *See, e.g.*, Central America–Dominican Republic Free Trade Agreement art. 15.10.1, May 28, 2004, *available at* https://ustr.gov/sites/default/files/uploads/agreements/cafta/asset_upload_file934_3935.pdf; United States–Australia Free Trade Agreement, U.S.–Austl., art. 17.10.1, May 18, 2004, *available at* https://ustr.gov/sites/default/files/uploads/agreements/fta/australia/asset_upload_file469_5141.pdf; United States–Singapore Free Trade Agreement, U.S.–Sing., art. 16.8.1, May 6, 2003, *available at* https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf.

62 TRIPS Agreement art. 39.3.

63 Weissman, *supra* note 26, at 166.

64 TRIPS Agreement art. 39.3.

in, the collected data.[65] Third, although Article 39.3 protects these data against "disclosure," it does not expressly prohibit regulatory authorities from making use of or relying on the data, such as when the data are used in conjunction with the bioequivalence studies submitted by generic drug manufacturers.[66] Finally, Article 39.3 anticipates the need for disclosure when it is "necessary to protect the public."[67] The provision therefore includes a built-in exception.

The existence of these many limitations is understandable, considering that undisclosed information "has never been the subject of any multilateral agreement before"—an observation aptly made by Jayashree Watal, a former TRIPS negotiator for India who now works in the WTO Intellectual Property Division.[68] Given the novelty of this multilateral arrangement, it is no surprise to find compromise language in Article 39.3. Such language not only reflects the developed countries' failure to achieve consensus during the TRIPS negotiations,[69] but also foretells the immense and ongoing challenge of developing greater international protection of trade secrets and proprietary data.

---

65 *See* COMM'N ON INTELLECTUAL PROP. RIGHTS, INTEGRATING INTELLECTUAL PROPERTY RIGHTS AND DEVELOPMENT POLICY: REPORT OF THE COMMISSION ON INTELLECTUAL PROPERTY RIGHTS 50 (2002) ("TRIPS does not require the imposition of data exclusivity, as such, on these test data, only protection against unfair commercial use."); Pugatch, *supra* note 26, at 129 ("The TRIPS Agreement currently provides the weakest level of data-exclusivity protection."); Reichman, *supra* note 26, at 141–42 ("[T]he meaning of 'unfair commercial use' will depend upon the kind of practices that domestic and foreign trade secret laws have traditionally regarded as unfair.").

66 *See* Frederick M. Abbott, *The Cycle of Action and Reaction: Developments and Trends in Intellectual Property and Health*, *in* NEGOTIATING HEALTH, *supra* note 26, at 27, 30 ("The TRIPS Agreement provides a limited form of protection for submissions of regulatory data; but this protection does not prevent a generic producer from making use of publicly available information to generate bioequivalence test data."); Reichman, *supra* note 26, at 144 ("Article 39.3 of the TRIPS Agreement does not prevent governments from relying upon decisions to allow the production of relevant products in other jurisdictions, nor does it prevent Members from authorizing the manufacture of bioequivalent products on the basis of positive regulatory decisions by local authorities. Legislative history, competition policy and sound principles of treaty interpretation support this conclusion, as do important decisions in two domestic courts."); *cf*. Pugatch, *supra* note 26, at 100 (defining non-reliance as the effort "to prevent the authorities themselves from relying upon the original registration file for a drug when comparing it to the chemical and toxic levels of a potential generic substitute (so-called bioequivalence tests)").

67 TRIPS Agreement art. 39.3.

68 JAYASHREE WATAL, INTELLECTUAL PROPERTY RIGHTS IN THE WTO AND DEVELOPING COUNTRIES 4 (2001).

69 *See* EUROPEAN COMMISSION, COMPULSORY LICENSING AND DATA PROTECTION 19 (2001), *available at* http://trade.ec.europa.eu/doclib/docs/2006/may/tradoc_122031.pdf ("It must be admitted that the wording of Article 39.3 does not, from a *prima facie* reading, appear to impose data exclusivity during a certain period of time. This lack of clarity is the obvious result of a difficult negotiation process where divergences of views arose between developing and industrialised countries as to the necessity of EC/US like type of data protection as well as among industrialised countries on the length of the data exclusivity period."); *see also* Sandeen, *supra* note 37, at 539–52 (discussing the different phases of the negotiations surrounding Article 39 of the TRIPS Agreement).

E. *Human Rights Organizations*

The final narrative highlights the concerns of human rights organizations, which have actively participated in the U.S.–China debate. Although intellectual property industries have always taken the position that the intellectual property system has successfully internalized the protection of human rights,[70] human rights organizations, commentators, and activists beg to differ. For example, in the *Statement on Intellectual Property Rights and Human Rights* released in August 2000, the U.N. Sub-Commission on the Promotion and Protection of Human Rights reminded governments of "the primacy of human rights obligations over economic policies and agreements."[71] A year later, the U.N. High Commissioner for Human Rights released a highly critical report on the many human rights challenges created by the TRIPS Agreement.[72] In a recent article, I also underscored the tensions, conflicts, and other impediments that bilateral, regional, and plurilateral trade agreements have posed to greater protection of human rights.[73]

More specifically for our discussion, there is an "uncertain grey line between state secrets and trade secrets."[74] From a human rights standpoint, the failure to appreciate the challenge of drawing this line has serious consequences. Only recently, American policymakers, businesses, and press expressed concern about the trial (and later conviction) of Peter Humphrey and his wife, both of whom had been accused of illegally acquiring private personal information during their investigation for GlaxoSmithKline.[75] A few years ago, the Australian government, businesses, and press also criticized China's heavy-handed

---

[70] For the Author's earlier discussions on the tension between intellectual property and human rights, see generally Peter K. Yu, *Digital Copyright Enforcement Measures and Their Human Rights Threats*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND INTELLECTUAL PROPERTY 455 (Christophe Geiger ed., 2015); Peter K. Yu, *Intellectual Property and Human Rights in the Nonmultilateral Era*, 64 FLA. L. REV. 1045 (2012) [hereinafter Yu, *Nonmultilateral Era*]; Peter K. Yu, *Reconceptualizing Intellectual Property Interests in a Human Rights Framework*, 40 U.C. DAVIS L. REV. 1039 (2007); Peter K. Yu, *Ten Common Questions About Intellectual Property and Human Rights*, 23 GA. ST. U. L. REV. 709 (2007).

[71] Intellectual Property Rights and Human Rights, Sub-Comm'n on the Promotion & Prot. of Human Rights Res. 2000/7, ¶ 3, U.N. Doc. E/CN.4/Sub.2/RES/2000/7 (Aug. 17, 2000).

[72] U.N. High Comm'r for Human Rights, *The Impact of the Agreement on Trade-Related Aspects of Intellectual Property Rights on Human Rights: Rep. of the High Comm'r*, ¶ 11, U.N. Doc. E/CN.4/Sub.2/2001/13 (June 27, 2001).

[73] *See* Yu, *Nonmultilateral Era*, *supra* note 70, at 1075–91 (discussing these conflicts, tensions, and impediments).

[74] Xiong Ping & Philip Griffith, *Protecting Trade Secrets in China: History and Context*, 4 QUEEN MARY J. INTELL. PROP. 30, 55 (2014).

[75] *See* Jane Perlez, *China Reveals Charges for British-American Couple in Case Involving Glaxo*, N.Y. TIMES, July 15, 2014, at B7 (reporting the charges); David Barboza, *In China, British Investigator Hired by Glaxo, and Wife, Are Sent to Prison*, N.Y. TIMES, Aug. 9, 2014, at B3 (reporting the convictions).

treatment of four Rio Tinto employees, who were initially accused of espionage and stealing state secrets but were later charged with and convicted of bribery and trade secret theft.[76]

Indeed, the foreign criticisms in the state secret area are often incompatible with those in the trade secret area. More troubling, both sets of criticisms tend to overlook the historical fact that trade secrets originated in China as a form of state secret.[77] Because state-owned enterprises, and by extension the state, were often involved in the early days of trade secret protection in China, the roots of such protection diverged significantly from those found in Australia or the United States.

To be certain, one could still debate about whether the Chinese state secret law is vague and arbitrary or whether it has been unfairly applied to foreign nationals, such as the Humphreys or the four Rio Tinto employees.[78] It is also important to question whether the line between business secrets and state secrets has been properly drawn in China, given the very different nature of the secret information involved. Regardless of one's position in these debates, however, it is not difficult to notice the unconvincing and self-serving positions taken by foreign governments, businesses, and media. To many foreign critics, whether the protection of secret information in China should be strengthened or weakened depends largely on whether the law protects their own interests.

II. FIVE MODEST SUGGESTIONS

Given the highly sensitive and polarized nature of the U.S.–China debate and the depth of the problem concerning online hacking, data breaches, and trade secret protection, this Article does not attempt to

---

76 *See* David Barboza, *Chinese Court Hands Down Stiff Sentences to Four Mining Company Employees*, N.Y. TIMES, Mar. 30, 2010, at A4 ("The four [Rio Tinto employees] were arrested last July on suspicions of espionage and stealing state secrets from Chinese state-owned steel companies. But after protests from Australian officials and foreign executives about the seriousness of the espionage accusations, the men were formally charged with bribery and stealing commercial secrets, which are lesser charges.").

77 *See* SHAN, *supra* note 29, at 4 (stating that, prior to China's re-opening in the late 1970s, "trade secrets were confined to being classified only as one important type of State secret and by that measure alone they acquired the status of State secrets and were protected by state administrative measures" (footnote omitted)). Even today, "[s]tate secrets can . . . include trade secrets that concern state security and state interests that have been determined by special legal procedures and that have been acknowledged by certain persons at a particular time." *Id.* at 138.

78 *See* David Barboza, *China Says Australian Is Detained in Spy Case*, N.Y. TIMES, July 10, 2009, at A10 ("Legal scholars noted that China's state secrets law was vague and is often used to punish political opponents or those Beijing considered a threat to national interests. . . . 'The reason it's up for revision is there's widespread dissatisfaction with it,' said Jerome Cohen, a professor of law at New York University and a specialist in China's legal system. 'It lends itself to arbitrary treatment. Police can take advantage of stretching the law.'").

identify the needed legal and policy reforms. Instead, this Part outlines five modest suggestions on how a more constructive debate can be developed to narrow the differences between China and the United States. In doing so, it seeks to identify ways to reduce online hacking and data breaches as well as to enhance the protection of trade secrets and proprietary data.

First, as far as the debate on China's effort to steal trade secrets and proprietary data is concerned, it is important to be more specific about the type of secret involved. Does the debate concern state secrets, political secrets, military secrets, personal secrets, scientific or technological secrets, or business, industrial, or trade secrets?

Obviously, the U.S. government and businesses care about the theft of more than one type of secret. In fact, they may care about the protection of *all* types of secrets. Nevertheless, different types of secrets implicate disparate laws and policies. Not only may the justifications for these laws and policies differ, their strengths and weaknesses may also vary. In addition, distinctive exceptions, limitations, and safeguards may have been built into the implicated laws and policies.

Thus, the more we can pinpoint the type of secret involved, the easier it will be to improve our understanding of the complicated issues, and the more likely we will be able to develop a well-reasoned debate. A more specific focus and a more concrete discussion will also help policymakers, commentators, and businesses to locate the solutions needed to address the ongoing challenge.

The second suggestion concerns the need to update the international standards for protecting trade secrets and other undisclosed information. The TRIPS Agreement—Article 39, in particular—was drafted based on standards available in the late 1980s and the early 1990s. As Daniel Gervais, who was working at the GATT/WTO Secretariat at the time of the TRIPS negotiations, observed, "TRIPS adjusted the level of intellectual property protection to what was the highest common denominator among major industrialized countries as of 1991."[79] It is therefore no surprise that many Chinese and U.S. businesses have found the TRIPS standards for the protection of trade secrets and undisclosed information inadequate.

Nevertheless, until the international community, or at least China and the United States,[80] can agree on new international minimum

---

[79] Daniel J. Gervais, *The TRIPS Agreement and the Doha Round: History and Impact on Economic Development*, *in* 4 INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE 23, 43 (Peter K. Yu ed., 2007).

[80] *Compare* C. FRED BERGSTEN ET AL., CHINA'S RISE: CHALLENGES AND OPPORTUNITIES 25 (2008) (noting the need for China and the United States to "develop a very informal but increasingly effective 'G-2' . . . to help guide the global governance process on an increasing number of economic topics"), *with* STEFAN A. HALPER, THE BEIJING CONSENSUS: HOW CHINA'S AUTHORITARIAN MODEL WILL DOMINATE THE TWENTY-FIRST CENTURY 216–18 (2010) (arguing against the elevation of the U.S.–China relations to the bilateral status of a special G-2

standards, it is unlikely that the dispute between China and the United States can be easily resolved. Although amending the TRIPS Agreement provides the most obvious path to revise these standards, the standards can also be modified through the negotiation of new bilateral, regional, and plurilateral agreements, such as the Anti-Counterfeiting Trade Agreement and the Trans-Pacific Partnership Agreement. Because China has thus far been excluded from the negotiation of these agreements,[81] it remains to be seen what other opportunities exist for these two countries to reach an agreement on the new standards for trade secrets and proprietary data.

The third suggestion regards the need for the U.S. government and American businesses to identify the specific deficiencies in current Chinese law, as opposed to making only vague criticisms. For illustrative purposes, consider the USTR's discussion of the Law Against Unfair Competition in his *2014 Section 301 Report*:

> Under Chinese law . . . available remedies are difficult to obtain, given that civil, administrative, and criminal enforcement against trade secrets theft remains severely constrained. Enforcement obstacles include various deficiencies in China's AUCL [Law Against Unfair Competition]; constraints on gathering evidence for use in litigation; difficulties in meeting the criteria for establishing that information constitutes a trade secret; and criminal penalties that do not provide adequate deterrents. Unlike other Chinese [intellectual property] laws, the AUCL does not expressly authorize judges to issue certain provisional orders that are often critical to the successful pursuit of a civil enforcement action. While China's new Civil Procedure Law may address, or partially address, that problem, there has been insufficient time to ascertain whether this new law is facilitating access to civil remedies in practice. Additionally, the AUCL appears to apply primarily to "commercial undertakings" and not to impose liability on individual actors; the AUCL also requires that a trade secret have "practical applicability," which may limit the scope of protection for early stage research.[82]

While the last sentence in this excerpt provides concrete suggestions for trade secret reform in China, the second sentence does not. The USTR is right to point out the many enforcement obstacles in China. However, the discussion of these obstacles has existed for more than two decades.[83] If they cannot be removed in the copyright, patent, and trademark areas, why would the situation be any different for trade

---

relationship).

[81] *See* Peter K. Yu, *TPP and Trans-Pacific Perplexities*, 37 FORDHAM INT'L L.J. 1129, 1132–51 (2014) (discussing China's experience as a "TPP outsider").

[82] 2014 SPECIAL 301 REPORT, *supra* note 24, at 32.

[83] *See* Agreement Regarding Intellectual Property Rights, Feb. 26, 1995, China–U.S., 34 I.L.M. 881 (providing in the annex an "Action Plan for Effective Protection and Enforcement of Intellectual Property Rights").

secrets?[84] Moreover, enforcement obstacles implicate areas that are both relevant and irrelevant to intellectual property protection. For similar reasons, "constraints on gathering evidence"[85] pose challenges to all forms of litigation. Even if Chinese intellectual property policymakers are sympathetic to the concerns of the USTR and American businesses, it is unclear how easy it would be for these policymakers to address issues that go beyond their mandate and field of expertise.

The fourth suggestion relates to our need to develop a holistic and more contextualized debate on the protection of trade secrets and proprietary data—perhaps by taking into account the economic, social, and cultural aspects of such protection. As much as laws and policies are needed to improve the protection of undisclosed proprietary information, we also need to think more about whether those laws and policies would respond to the divergent local business, employment, and cultural conditions. In a recent book, Catherine Fisk wrote: "As workplace knowledge became corporate intellectual property, the combination of new legal and business practices transformed not only work relations but also class relations for creative people."[86] In her view, the protection of trade secrets, proprietary data, and workplace knowledge concern not only rights holders, but also other people involved.

In a very crowded environment such as China, it is not always easy to protect trade secrets and other confidential information, not to mention that many Chinese are still accustomed to using inside knowledge to show connections, earn respect, enhance stature, or indicate actual power or influence.[87] The protection of trade secrets also goes hand in hand with the reasonable measures taken to maintain secrecy. Article 39.2 of the TRIPS Agreement specifically mentions the "reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[88] In many jurisdictions, courts determine the grant of trade secret protection based on whether the right holders have taken reasonable security measures.[89] Given the requirement of having these measures and the inevitable variations over

---

84 *See* Daniel C.K. Chow, *Navigating the Minefield of Trade Secrets Protection in China*, 47 VAND. J. TRANSNAT'L L. 1007, 1011 (2014) ("[T]rade secrets are notoriously difficult to enforce in China and present obstacles that are in some important respects even greater than hurdles in the enforcement of other intellectual property rights, such as trademarks.").

85 2014 SPECIAL 301 REPORT, *supra* note 24, at 32.

86 CATHERINE L. FISK, WORKING KNOWLEDGE: EMPLOYEE INNOVATION AND THE RISE OF CORPORATE INTELLECTUAL PROPERTY, 1800–1930, at 245 (2009).

87 *Cf.* HAROLD CHEE WITH CHRIS WEST, MYTHS ABOUT DOING BUSINESS IN CHINA 65–74 (2d ed. 2007) (discussing the myth and reality about the use of "guanxi," or connections, in China).

88 TRIPS Agreement art. 39.2(c).

89 For a discussion of the need for these measures, see generally Robert G. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions*, *in* TRADE SECRECY HANDBOOK, *supra* note 37, at 46.

what measures would be deemed reasonable in the circumstances,[90] it is logical to question whether the trade secrets protected in one country would automatically be protected in another.

The final suggestion pertains to our need to develop a deeper and more sophisticated understanding of information flow. This flow involves not only trade secrets and proprietary data, but also all other types of information. Developing such an understanding is important, because the flow of information, like water or heat, is often hard to control. As Hans von Baeyer put eloquently:

> As humans, we not only acquire information through our senses, we also feel compelled to share it with each other. From the first cries of emerging humans that we hear echoed from a baby's crib, from the gossip of cave-dwellers around the communal fire to our satellite-transmitted e-mail messages, the appetite for information has been as integral to the human condition as the hunger for food and love.[91]

Thus, instead of focusing on preventing the flow of information—through legal protection or otherwise—it is increasingly important to reframe the debate as one about risk management and damage mitigation.[92]

While some would certainly fear that the information flowing to China could harm the United States—by, perhaps, undermining the latter's competitive advantage—the same flow of information could also create opportunities while promoting collaboration between Chinese and U.S. businesses. After all, businesses are unlikely to work with each other if they do not understand what others are doing or if their approaches are vastly different.

At the macro level, an active flow and exchange of information is also important because it can help improve or stabilize the oft-turbulent U.S.–China relationship. As Zhou Enlai, the former Chinese premier, once told Henry Kissinger, "When you have become familiar with [China], it will not be as mysterious as before."[93] Richard Clarke and Robert Knake concurred: "Knowing what another nation's capabilities are and having a view into what they are doing behind closed doors

---

90 *See* Sandeen, *supra* note 37, at 557 ("In practice, what is reasonable depends upon an analysis that is partly based upon the facts and partly upon the court's perception of fairness. In effect, the reasonable efforts requirement encompasses the 'general principles' approach initially proposed by the EC because it allows WTO member countries latitude to determine what is reasonable in light of their own definitions of honest and dishonest commercial practices.").

91 HANS CHRISTIAN VON BAEYER, INFORMATION: THE NEW LANGUAGE OF SCIENCE 9 (2003).

92 *See* Bambauer, *supra* note 40, at 1019 ("[F]ocusing efforts principally on preventing cyberattacks is misguided: perfect security is impossible, and even attaining good security is extraordinarily difficult. Instead, cybersecurity regulation should concentrate on mitigating the damage that successful attacks cause.").

93 RICHARD H. SOLOMON, CHINESE NEGOTIATING BEHAVIOR: PURSUING INTERESTS THROUGH "OLD FRIENDS" 15 (1999).

usually contributes to stability."[94]

In sum, the flow of information does not always harm a country; it depends on the type of information involved. To avoid throwing away the baby with the bath water, we need to develop a deeper and more sophisticated understanding that separates the good flow of information from its bad flow. In doing so, we will be able to focus more on risk and damage than on protection per se. While some information should be protected, other should be allowed to flow freely.

CONCLUSION

This Article has shown how the parties in the current U.S.–China debate on online hacking and trade secret protection continue to talk past each other. To help identify reform options that benefit both sides, the Article offers five modest suggestions on how a more positive debate can be constructed. Although these suggestions will in no way resolve the ongoing dispute between China and the United States, it is my hope that they will provide an important step toward strengthening the protection of trade secrets and proprietary data in China.

Policymakers, commentators, and the media remain fascinated by the potential conflict between Chinese culture and intellectual property reforms—a proposition other commentators and I have repeatedly questioned.[95] Trade secrets, however, is not an area in which such a conflict has arisen. In this area, China and the United States actually share some common and historical interests.

In China, the efforts to protect workplace knowledge and technical information date back to centuries ago. During the Qing Dynasty, for example, "the producers of the celebrated Tongren Temple line of medicines . . . sought to maintain the confidentiality of their manufacturing process by employing only family members or eunuchs, or by keeping vital parts of the process secret from nonfamily employees."[96] Given this longstanding tradition and the common interests between China and the United States, it is indeed lamentable that these two countries have thus far failed to work more closely together to strengthen the protection of trade secrets and proprietary data. Such strengthened protection would benefit not only American businesses but also Chinese industries.

---

94 CLARKE & KNAKE, *supra* note 10, at 230.

95 For the Author's recent discussions on Confucianism and intellectual property reforms, see generally Peter K. Yu, *Intellectual Property and Confucianism*, *in* DIVERSITY IN INTELLECTUAL PROPERTY: IDENTITIES, INTERESTS, AND INTERSECTIONS 247 (Irene Calboli & Srividhya Ragavan eds., 2015); Peter K. Yu, *The Confucian Challenge to Intellectual Property Reforms*, 4 WIPO J. 1 (2012).

96 WILLIAM P. ALFORD, TO STEAL A BOOK IS AN ELEGANT OFFENSE: INTELLECTUAL PROPERTY LAW IN CHINESE CIVILIZATION 16 (1995).