

COMMENTS

OF PROTECTION AND SOVEREIGNTY: APPLYING THE COMPUTER FRAUD AND ABUSE ACT EXTRATERRITORIALLY TO PROTECT EMBEDDED SOFTWARE OUTSOURCED TO CHINA

CARRIE GREENPLATE*

TABLE OF CONTENTS

Introduction.....	130
I. Overview of Business Arrangements and Choice of Law When Offshore Sourcing to China.....	136
A. Joint Ventures and Wholly Foreign-Owned Enterprises Are Most Popular.....	136
B. Choice of Law and Choice of Forum Depend on the Offshore Sourcing Arrangement.....	138
II. Chinese and U.S. Regulatory Law Are Insufficient to Provide Protection to U.S. Citizens and Companies	141
A. Chinese Law Does Not Restrict Exporting Products Containing Embedded Software.....	142
B. U.S. Laws Focus on National Defense	143
III. The Computer Fraud and Abuse Act Is A Means To Enhance Security.....	146
A. The Computer Fraud and Abuse Act Encompasses Malicious Code in Embedded Software	147

* Note and Comment Editor, *American University Law Review*, Volume 57; J.D. Candidate, May 2008, *American University, Washington College of Law*; B.S. in Business Administration, 1998, *John Carroll University*. I would like to thank my editor Tritia Yuen and Professors Padideh Ala'i and Mary Clark for their reviews and suggestions throughout the writing process. Thank you to my parents, William and Julia, for teaching me the value of hard work. Finally, to my partner and soul mate, Juan Amezcua, thank you for your unconditional love and support always.

B. The U.S. Company Should Choose U.S. Law or Incorporate the CFAA Language into Private Contracts.....	155
C. Using the Extraterritoriality of the CFAA to Enforce Security in Offshore Sourcing Situations.....	155
1. The CFAA statutory language and legislative history show intent for its extraterritorial application.....	158
2. The effects test allows a court to extend the CFAA extraterritorially.....	160
3. The conduct test may also be used to find subject matter jurisdiction.....	166
D. International Comity Considerations Support Subject Matter Jurisdiction.....	170
1. The jurisdictional rule of reason approach leads to exercising subject matter jurisdiction.....	171
2. Policy considerations also permit exercising jurisdiction.....	174
Conclusion.....	177

INTRODUCTION

Cars, airplanes, compact disc players, cellular telephones, heart monitors, weapons systems, and personal computers all have it.¹ In “the race to the bottom,” an ever increasing number of U.S. businesses turn to the People’s Republic of China (“China”) to develop it.² But, the United States Government,³ and some

1. Edward A. Lee, *Embedded Software*, Nov. 1, 2001, <http://ptolemy.eecs.berkeley.edu/publications/papers/02/embssoft/embssoftwre.pdf>, published in 56 ADVANCES IN COMPUTERS 56 (2002) [hereinafter Lee, *Embedded Software*]; accord Bas Graaf et al., *Embedded Software Engineering: The State of the Practice*, IEEE SOFTWARE, Nov.-Dec. 2003, at 61 (reiterating that cars and airplanes as well as DVD players and medical systems use embedded software); Edward A. Lee, *What’s Ahead for Embedded Software?*, COMPUTER, Sept. 2000, at 18 [hereinafter Lee, *What’s Ahead*] (repeating that “gadgets and cars use embedded software”).

2. See Stephen F. Diamond, *The “Race To The Bottom” Returns: China’s Challenge To The International Labor Movement*, 10 U.C. DAVIS J. INT’L L. & POL’Y 39, 41-42 (2003) (describing the “race to the bottom” not solely in terms of a company’s ability to employ the lowest wages but also its ability to combine high-productivity with lower wages than would be demanded in more developed countries); see also Paul McDougall, *The Offshore Equation*, INFO. WEEK, Sept. 6, 2004, at 32, available at <http://www.informationweek.com> (search “The Offshore Equation”) (providing an example of a moving and relocation company who required a Return on Investment within two years; to meet this ROI and provide a technical solution to better match customer demand with available trucks, the company had to use a software development company based in India, at a fraction of the cost).

3. See Mickey Meece, *Lenovo Aims to Calm Fears Over Security*, N.Y. TIMES, July 29, 2006, at C3 (reporting on the State Department’s fears of viruses in computers purchased from Lenovo, a China-based computer manufacturer); Gary Anthes, *DOD Report to Detail Dangers of Foreign Software*, COMPUTERWORLD, Nov. 22, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=274599&intsrc=hm_list (announcing that one day, the United States will “badly

independent researchers⁴ are concerned about the vulnerability of it. “It” is embedded software—the instructions that programmers encode within a device, such as a CD player or weapon system, that help the device function.⁵

Embedded software pervades civilian and military products due to the increasing sophistication and use of technology.⁶ U.S. companies that develop this embedded software compete in a global market where labor and resource costs outside the United States are lower.⁷ Therefore, these companies choose to develop, or “source,”

need communications” and will have a denial of service attack resulting in a “billion-dollar weapon[] unable to function”); *see also* John R. Schmertz & Mike Meier, *U.S. Clears Merger of IBM’s PC Division with Giant Chinese Computer Maker*, 11 INT’L L. UPDATE 47, 47 (2005) (reporting that to complete the sale Lenovo agreed to move its headquarters from Beijing to the United States to satisfy the U.S. government).

4. *See* John Markoff, *Study Says Chips in ID Tags Are Vulnerable to Viruses*, N.Y. TIMES, Mar. 15, 2006, at C3 (quoting the opinion of Peter Neumann, a computer scientist at a research firm in California, who said “[i]t shouldn’t surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever”); Erik Sherman, *Going East*, INFO. SECURITY, Nov. 2003, at 14, *available at* http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss205_art458,00.html (emphasizing that the inclusion of malicious code is a risk when using third parties to code a company’s software); *see also* Richard Ford, *Malcode Mysteries Revealed*, SECURITY & PRIVACY (IEEE, New York, NY), May-June 2005, at 72 (reporting that viruses and worms still exist and should be defended against even though some computer users see them as requirements to the benefits of technology).

5. *See, e.g.,* Lee, *Embedded Software*, *supra* note 1, at 1 (stressing that embedded software’s principal role is its “interaction with the physical world” and its execution on various machines that are not necessarily personal computers).

6. *E.g.,* Graaf, *supra* note 1, at 61 (predicting that by 2013 the use of products containing embedded software will grow “exponentially”). Contrary to what its name might imply, embedded software is not simply typical software, such as Microsoft Word, on a microchip. Lee, *Embedded Software*, *supra* note 1, at 2. Embedded software is more closely related to the device or hardware into which it is programmed, such as a telephone or personal digital assistant (“PDA”), than Microsoft Word is related to a computer. *Id.* Microsoft Word can be used on many devices, including different brands of computers or PDAs, but embedded software programmed for a cellular telephone is suitable only for the telephone. As such, the hardware constrains the ability to program, test, and secure the embedded software. Graaf, *supra* note 1, at 61. Often an engineer who is an expert in the hardware designs the embedded software program, rather than a typical software programmer who can design and build a program for use on many different types of operating systems. Lee, *What’s Ahead*, *supra* note 1, at 19. Therefore, this Comment chooses to focus on embedded software because of its increasing use, its requirement for specialization, and its challenge to thorough testing.

7. *See, e.g.,* Carlos Grande, *Companies UK: Marconi’s Technology Fails the Price Test*, FIN. TIMES (London), May 4, 2005, at 23 (reporting that Marconi lost a British Telecom contract based on price, not knowledge, which might lead to a reduction in Marconi’s R&D workforce to reduce its own costs); Paul McDougall, *supra* note 2, at 32 (providing an example of a moving and relocation company that used a software development company based in India, at a fraction of the cost of software development companies in the United States, in order to meet a two-year Return on Investment).

embedded software offshore to decrease costs and increase profits quickly.

The term “offshore sourcing” refers to the situation where a company uses low cost, high quality labor in a “host” country to perform tasks or processes that are not part of the company’s core business.⁸ With over 5,000 students and professionals completing studies in the United States, then returning to China, more U.S. companies are choosing China as a host country because the high quality of the workforce in addition to its lower cost equals a high return on investment.⁹ Increasingly, however, this selection is causing

8. ERRAN CARMEL & PAUL TJIA, OFFSHORING INFORMATION TECHNOLOGY: SOURCING AND OUTSOURCING TO A GLOBAL WORKFORCE xix (2005) (using the term “offshore sourcing” to encompass the situation “[w]here sourcing can be from outside the firm or inside the firm[,]” but the location is outside the boundaries of the home country). In other words, the U.S. company has sourced a portion of work to a different country. *Id.* Offshore sourcing may also include joint ventures with a partner company that is local to the foreign country. *Id.* at 120 (reviewing the principle deal structures of an offshore sourcing arrangement, including the captive center/subsidiary, joint venture, build operate transfer model, and contract). *See generally* Trevor W. Nagel & Michael T. Murphy, *Structuring Technology Outsourcing Relationships: Customer Concerns, Strategies and Processes*, 4 INT’L J.L. & INFO. TECH. 151, 163 (1996) (noting that a proposal for outsourcing work can be a strategic alliance or partnership). Strictly speaking, “offshoring” signifies using a non-home country for a business transaction. CARMEL & TJIA, *supra*, at xviii; *see* Fraser Mendel, *Offshore Outsourcing and Offshoring to China*, in JOHN F. DELANEY & WILLIAM A. TANENBAUM, PRACTISING LAW INST., THE OUTSOURCING REVOLUTION 2005: PROTECTING CRITICAL BUSINESS FUNCTIONS 257 (2005) (defining “offshore outsourcing” as hiring a third-party to complete work for the customer’s business “in a country other than the one that is the major market for the final product or service”). Correspondingly, businesses use “outsourcing” to signify “that tasks and processes are contracted to be performed outside the boundaries of the firm.” CARMEL & TJIA, *supra*, at xviii-xix (elaborating with the example that General Electric uses Tata Consultancy Services in India to perform certain tasks, while Siemens has a center it owns in India). Additionally, businesses use the term to signify when they delegate an entire process, and sometimes physical assets or staff, to an outsider. *Id.* at xviii-xix (providing the example that these processes can be a single task for a one time project or an ongoing business process such as a call center). *See generally* E. Michael Power & Roland L. Trope, *Averting Security Missteps in Outsourcing*, <http://www.computer.org/security> (describing how companies increasingly use providers in other countries to perform tasks on a continuing basis). This Comment uses the terms “offshore sourcing” and “sourcing” to mean performing some business task in a non-U.S. country.

9. CARMEL & TJIA, *supra* note 8, at 31 (comparing the average annual wage for a software professional in the United States of \$63,000 with \$9,000 at the highest range for India and \$14,200 at the highest range for China). Furthermore, the Chinese Communist Party declared in their Tenth Five-Year Plan in 2001 that developing skills in technology is a key goal for the country. Tenth Five-Year Plan for National Economic and Social Development (promulgated by State Council of China, Mar. 15, 2001, effective Mar. 15, 2001), *translated at* <http://www.trp.hku.hk/infofile/china/2002/10-5-yr-plan.pdf> (last visited Aug. 27, 2007) (P.R.C.) [hereinafter Tenth Five-Year Plan P.R.C.] (listing “Making Reform and Opening Up and Making Technological Progress the Driving Force” as one of the Guiding Principles of the Five-Year Plan). As stated in its 1982 Constitution and in its Tenth Five-Year Plan, China is committed to opening the country to investment and in particular wants to develop its technology sector. XIAN FA preamble (1982) (P.R.C.); Tenth Five-Year

concerns about the security of the resulting embedded software product.¹⁰

In 2005, the Department of Defense (“DOD”) commissioned a Defense Science Board Task Force to study “the extent to which foreign influenced software is embedded within systems critical to [its] mission”¹¹ Although the government commissioned the study, any industry using embedded software feels this foreign influence due to the complexity and globalization of computer software.¹² For example, a group of independent researchers demonstrated that a programmer could insert a software virus into a radio frequency identification tag (“RFID”), which is part of a microchip-based tracking technology used in commercial applications.¹³

Plan P.R.C., *supra*. See generally U.S. GOV’T ACCOUNTING OFFICE, OFFSHORING: U.S. SEMICONDUCTOR AND SOFTWARE INDUSTRIES INCREASINGLY PRODUCE IN CHINA AND INDIA 2, 8-12 (2006) (tracking the flow of manufacturing of semiconductor devices and software development to India and China from the early 1990s and summarizing that the cost savings and high quality work companies experienced overseas led companies to expand offshore sourcing to software and systems integration).

10. See Power & Trope, *supra* note 8, at 70-73 (discussing the security risks posed by outsourcing technology development to outsiders).

11. See Memorandum from Kenneth J. Krieg, Under Secretary of Defense, to Chairman, Defense Science Board (Oct. 5, 2005), <http://www.acq.osd.mil/dsb/tors/TOR-2005-10-05-MIFIDS.pdf>; see also DEFENSE SCIENCE TASK FORCE, HIGH PERFORMANCE MICROCHIP SUPPLY 3 (2005), available at <http://www.acq.osd.mil/dsb/reports/2005-02-HPMS%5FReport%5FFinal.pdf> (summarizing that the study revealed that the manufacturing capabilities of critical microelectronics have moved to countries with lower cost capital, which results in lower trustworthiness and supply assurance for such components); Anthes, *supra* note 3 (discussing the upcoming release of the DOD report that “calls for a variety of prevention and detection measures”). According to the Anthes article, the DOD task force was supposed to de-classify the full software report in early 2007. *Id.* As of July 1, 2007, the report is not posted. When de-classified, the report will be available at the Defense Science Board website, <http://www.acq.osd.mil/dsb/reports.htm>.

12. Anthes, *supra* note 3 (clarifying that it is not xenophobia but the fact that everything is connected that makes networks vulnerable to code that is developed overseas with little or no U.S. oversight); accord Sherman, *supra* note 4, at 14 (discussing concerns from companies and academic researchers regarding the vulnerability of software developed overseas).

13. Markoff, *supra* note 4. In addition, experts in the computer engineering field report that ensuring fully secure embedded software—meaning little to no software errors—is, at best, difficult. *E.g.*, PAUL KOCHER ET AL., SECURITY AS A NEW DIMENSION IN EMBEDDED SYSTEM DESIGN 753 (2004) (asserting that although security for embedded software systems is critical, these same systems are constrained by their own designs from providing full security); Louise Longdin, *Liability for Defects in Bespoke Software: Are Lawyers and Information Scientists Speaking the Same Language?*, 8 INT’L J.L. & INFO. TECH. 1, 11 (2000) (reporting that often software is released with known defects).

The cost of failed software can be in the billions of dollars.¹⁴ Even more devastating, it can result in the loss of life. A Patriot Missile failed to intercept an Iraqi Scud missile during the 1991 Gulf War, killing twenty-eight American soldiers, because the missile's software contained incorrect calculations.¹⁵ While that was an inadvertent miscalculation, programmers can insert malicious miscalculations into any embedded software developed overseas.¹⁶ This malicious code can be a virus, worm, or any other series of computations that would cause a harmful effect to the product or the product's user.¹⁷

Although companies test embedded software before releasing the product to the buyer, the amount of testing varies and at best only guarantees that the product has less than a certain number of defects, not zero defects.¹⁸ As a result, companies could unknowingly release products containing a malicious code. Different political regimes and possible animosity towards the United States increase this risk.¹⁹

This Comment argues that the United States has the legal means to address the challenges presented by sourcing embedded software

14. *E.g.*, James Gleick, *Little Bug, Big Bang*, N.Y. TIMES, Dec. 1, 1996, § 6 (Magazine), at 38 (reporting on the crash of the Ariane-5 unmanned rocket that cost \$7 billion to build and explaining that an incorrect conversion of a 64-bit number to a 16-bit number caused the system to shut down and the rocket to explode on its first launch).

15. U.S. GEN. ACCOUNTING OFFICE, PATRIOT MISSILE DEFENSE: SOFTWARE PROBLEM LED TO SYSTEM FAILURE AT DHAHRAN, SAUDI ARABIA I (1992).

16. *See, e.g.*, Anthes, *supra* note 3 (quoting Ira Winkler, author of the book *Spies Among Us*, as suggesting that “[i]f there is one line of code written overseas, that’s one line too many”).

17. *See* Ford, *supra* note 4, at 72 (defining viruses and worms). People often use the terms virus and worm interchangeably. However, they are technically different. A virus is a self-replicating program that copies itself and can modify other programs, such that using the modified program implies using an evolved version of the original virus. *Id.* at 72. On the other hand, a worm is a self-contained program that does not need other programs in order to copy itself to other computer systems. EUGENE H. SPAFFORD, A FAILURE TO LEARN FROM THE PAST 2 (2003). Regardless, both a virus and a worm can be classified as malicious code. *Id.* *See generally* Symantec Corp., What Is The Difference Between Viruses, Worms, and Trojans?, <http://service1.symantec.com/SUPPORT/nav.nsf/docid/1999041209131106> (last visited Aug. 19, 2007) (providing more definitions of various malicious programs).

18. *See, e.g.*, Longdin, *supra* note 13, at 10-11 (relating the various methods of testing, including user acceptance testing, that most software goes through). Some software manufacturers may use “cleanroom” engineering to certify reliability. *Id.* at 10. “Cleanroom” engineering means that throughout the entire program development process the quality of the product is continually assessed and, if necessary, adjusted. *Id.* While this results in fewer errors, it is also time intensive, resulting in higher development costs. *Id.* at 10-11.

19. *E.g.*, U.S. GEN. ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS 14 (2004) (concluding that the security of the control system that governs U.S. infrastructure is vulnerable to cyber-attacks); Robert Lezner & Nathan Vardi, *The Next Threat*, FORBES, Sept. 20, 2004, at 70 (reporting that the FBI and NSA believe foreign governments such as Iran and China have trained hackers in Internet warfare).

development in China. This Comment uses an “embedded software scenario” as its example for analysis of the risks involved in developing embedded software in China and the possible legal means to reduce that risk or prosecute the offenders.²⁰

In the embedded software scenario, a U.S. company uses China as a host country and Chinese employees to develop embedded software for any number of devices. Thus, in the scenario, it is a Chinese programmer who inserts malicious code into the embedded software.²¹ The U.S. company then exports the embedded software from China to the United States, where the malicious code executes and damages the end-user. Part I explains the two business arrangements the U.S. company likely uses when offshore sourcing to China. Part I will also briefly analyze the U.S. company’s ability to choose the law and forum that will govern in the event of a breach of contract. This understanding is important because while Part II explains that Chinese and U.S. regulatory laws are not sufficient protection for the risks of the embedded software scenario, Part III suggests that parties to the contract should choose U.S. law where they have the freedom to do so or, alternatively, incorporate the language of the Computer Fraud and Abuse Act (“CFAA”)²² into private contracts as additional protection.²³ Finally, Part III argues that *United States v. Ivanov*²⁴ properly applied the CFAA extraterritorially and uses a comparison to extraterritorial application

20. Since the Internet, viruses have become mainstream. Correspondingly, many law review articles have been written on the question of jurisdiction. The majority of these articles focus on jurisdiction over the Internet for any country or jurisdiction over crimes that take place over the Internet; they do not generally discuss the extraterritorial application of the Computer Fraud and Abuse Act (“CFAA”). See, e.g., Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1, 3-10 (2004); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 2-5 (1996); Ellen S. Podgor, *Cybercrime: National, Transnational, or International?*, 50 WAYNE L. REV. 97, 97-101 (2004). One Note does apply the principles of extraterritorial jurisdiction to the 1994 version of the CFAA, but again does so generally to viruses released over the Internet. John Eisinger, Note, *Script Kiddies Beware: The Long Arm of U.S. Jurisdiction to Prescribe*, 59 WASH. & LEE L. REV. 1507, 1508, 1512-37 (2002). This Comment, in contrast, focuses on two jurisdictions, the United States and China. This Comment also does not address viruses released over the Internet. Instead, it focuses on a virus within a physical good such as a computer, car, or airplane and analyzes extraterritorial jurisdiction of the current CFAA in light of extraterritorial application of U.S. antitrust and securities laws.

21. Although any programmer, Chinese or American, could insert malicious code into embedded software, this Comment chooses to focus on the situation where a Chinese programmer does so in order to limit the paper to the territorial jurisdiction issues.

22. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, tit. II, ch. XXI, 98 Stat. 1837, 2190-92 (1984) (current version at 18 U.S.C. § 1030 (2000)).

23. See *infra* Part III (discussing the advantages to incorporating U.S. law into foreign contracts).

24. 175 F. Supp. 2d 367 (D. Conn. 2001).

of economic laws to support this argument. The article concludes that a U.S. court should find subject matter jurisdiction under the CFAA in the embedded software scenario, providing the United States with a method to deter and punish those who jeopardize the security of technological products.

I. OVERVIEW OF BUSINESS ARRANGEMENTS AND CHOICE OF LAW
WHEN OFFSHORE SOURCING TO CHINA

Sourcing business in China is a relatively new experience for most U.S. companies.²⁵ A U.S. company sourcing in China can choose from several types of business arrangements.²⁶ Two of the most popular are joint ventures and wholly foreign-owned enterprises (“WFOEs”).²⁷ Each business arrangement has different results regarding control of the business and choice of law and forum.

A. *Joint Ventures and Wholly Foreign-Owned Enterprises Are Most Popular*

A U.S. company interested in offshore sourcing to China can choose to be a foreign-invested enterprise with a Chinese partner through a joint venture.²⁸ In this arrangement, there is a contract

25. See JAMES M. ZIMMERMAN, CHINA LAW DESKBOOK: A LEGAL GUIDE FOR FOREIGN-INVESTED ENTERPRISE 81 (2d ed. 2004) (noting that 1980s regulations limited the types of direct investments businesses could undertake in China, but today China has relaxed some standards to make a wholly foreign-owned enterprise more common); US-China Business Council, An Introduction to the US-China Business Council, <http://www.uschina.org/more.html> (last visited July 23, 2007) (explaining that since the end of the 1970s, there has been “massive growth of U.S.-China economic engagement”). Even though international business transactions can be traced back to 1622, establishing a business in China has only recently become common. JOHN H. JACKSON ET AL., LEGAL PROBLEMS OF INTERNATIONAL ECONOMIC RELATIONS 46-48 (3d ed. 1995) (diagramming a “typical international sales transaction” and noting that international law may affect a bank’s ability to issue letters of credit and that “conflict of laws” arise during contractual disputes of this nature); Lee Peoples, *Strategies and Sources for International Legal Research*, 60 CONSUMER FIN. L.Q. REP. 412, 421 (2006) (noting that international trade law can be traced back to 1622 and the customary law of merchants).

26. See CARMEL & TJIA, *supra* note 8, at xix (reviewing offshore arrangements such as the subsidiary arrangement, joint venture, build operate transfer model, and one-time contracts for specific tasks); Nagel & Murphy, *supra* note 8, at 163 (noting that a proposal for outsourcing work can be a strategic alliance or partnership).

27. Jie Chen, *Guide to Establishing a Subsidiary in China*, THE LICENSING JOURNAL, Nov.-Dec. 2005, at 8.

28. CARMEL & TJIA, *supra* note 8, at 119; ZIMMERMAN, *supra* note 25, at 90, 103. For purposes of this Comment, the foreign partner has no possibility of acquiring a controlling interest in the joint venture or U.S. company. If the Chinese partner could acquire a controlling interest, the arrangement would be subject to review under the Exon-Florio Amendment. 50 U.S.C.A. app. § 2170 (1994); 31 C.F.R. 800.301; David Scott Nance & Jessica Wasserman, *Regulation of Imports and Foreign Investment in the United States on National Security Grounds*, 11 MICH. J. INT’L L. 926, 965-66 (1990); see Jose E. Alvarez, *Political Protectionism and United States International Investment Obligations in Conflict: The Hazards of Exon-Florio*, 30 VA. J. INT’L L. 1, 82-83

between the U.S. company and the Chinese counterpart to form the joint venture.²⁹ In addition, there are separate contracts for any transactions or agreements between the resulting joint venture enterprise and the U.S. company.³⁰ Similarly, there are contracts for transactions between the joint venture enterprise and the Chinese counterpart.³¹ While a joint venture gives some control of the business to the China-based partner, having a Chinese counterpart, who is more familiar with Chinese law, can be a significant benefit to the U.S. company.³²

Alternatively, a U.S. company can choose to be a foreign-invested enterprise without a China-based partner by creating its own center to develop the embedded software.³³ The U.S. company can consider this a branch of the U.S. office or a subsidiary of the parent company.³⁴ Under Chinese law this arrangement will usually create a

(1989); *infra* Part II.B (discussing the Exon-Florio Amendment). Joint ventures in China must be approved by the Ministry of Foreign Economic Relations and Trade. Regulations for the Implementation of the Law on Joint Ventures Using Chinese and Foreign Investment (promulgated by State Council, Sept. 20, 1983, effective Sept. 20, 1983), art. 8, *translated at* <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/1> (last visited Aug. 19, 2007) (P.R.C.) [hereinafter Regulations for Implementation of Joint Ventures P.R.C.].

29. See Regulations for Implementation of Joint Ventures P.R.C., *supra* note 28, at art. 9(1) (discussing the process of approval for a joint venture with a foreign entity).

30. See *id.* art. 7 (listing the various agreements and contracts that the joint ventures have the right to operate under).

31. *Id.*

32. The Chinese partner may be more connected in the government and judicial system, which can facilitate approvals and prompt treatment in the courts. ZIMMERMAN, *supra* note 25, at 89 (pointing out that a Chinese partner can assist in developing an operational base, securing resources, and using “guanxi” or “connections” to help with government approval); accord Patricia Pattison & Daniel Herron, *The Mountains Are High and the Emperor Is Far Away: Sanctity of Contract in China*, 40 AM. BUS. L.J. 459, 484-85 (stating that “guanxi” is a method of cultivating relationships and has often benefited Chinese citizens when the rule of law has been lacking). *But see* ZIMMERMAN, *supra* note 25, at 92 (asserting that WFOEs are more popular now and giving tips on how to select a Chinese partner if law or necessity does not allow the U.S. company to set up a WFOE).

33. CARMEL & TJIA, *supra* note 8, at 119. In China, the detailed regulations vary depending on the type of organization and parties involved. For example, China has a specific law for joint ventures and a different law for WFOEs. *E.g.*, Regulations for Implementation of Joint Ventures P.R.C., *supra* note 28; Detailed Rules for the Implementation of the Law on Wholly Foreign-Owned Enterprises in China (re-promulgated by Order No. 301 of the State Council, April 12, 2001, effective April 12, 2001) (P.R.C.), *translated at* <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/3> (last visited Sept. 10, 2007) [hereinafter Rules for Implementation of WFOEs P.R.C.]. Because state law generally governs businesses in the United States, the state in which the business operates or is incorporated would govern the type of offshore sourcing arrangement in the United States. See generally KONRAD ZWEIGERT & HEIN KOTZ, INTRODUCTION TO COMPARATIVE LAW 260-61 (Tony Weir trans., 3d rev. ed. 1998).

34. See CARMEL & TJIA, *supra* note 8, at xix, 119; see also Chen, *supra* note 27, at 7 (guiding readers on the value of establishing a subsidiary in China if the company intends to conduct long-term business in China). In either the captive center or

WFOE.³⁵ U.S. companies typically choose to establish a WFOE to have maximum control in hiring employees and dictating company policy, while enjoying limited liability.³⁶ Unlike a joint venture, there is no contract between the U.S. company and a Chinese counterpart in this arrangement.³⁷ Although the prospect of having a formal Chinese business partner affects the arrangement the U.S. company chooses, the ability to choose the law and the forum governing the contracts also affects the decision of the U.S. company to source development in China.³⁸

B. Choice of Law and Choice of Forum Depend on the Offshore Sourcing Arrangement

Just as U.S. parties to a contract can often choose which law and forum will govern any contractual disputes, China's Contract Law

subsidiary arrangement, the company could have started the business in China or acquired an already established company. CARMEL & TJIA, *supra* note 8, at 119. To analyze U.S. regulatory law in Part II.B, this Comment assumes that the foreign-based subsidiary or branch has no possibility of acquiring a controlling interest in the U.S. parent company.

35. Rules for Implementation of WFOEs P.R.C., *supra* note 33; ZIMMERMAN, *supra* note 25, at 76-80, 113; *cf.* Company Law (promulgated by Standing Committee of National People's Congress, Dec. 29, 1993, revised Dec. 25, 1999), ch. 9 (P.R.C.), translated at <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/1> (last visited Aug. 19, 2007) (allowing foreign companies to set up branches in China; however, different laws govern WFOEs or joint ventures). The arrangement could also be a representative office but this is less likely because a representative office may not engage in profit making activities, including signing contracts. *See* Chen, *supra* note 27, at 7 (commenting that while a representative office can act as a liaison for a foreign-based company, it cannot conduct business in China directly). Each of these are distinct types of "foreign invested enterprises" without a Chinese partner that are available to any foreign party. ZIMMERMAN, *supra* note 25, at 75. China also recognizes other business arrangements such as processing trade contracts, holding companies, and foreign-invested venture capital investment enterprises. *Id.* at 106-25. However, these types of organizations are not applicable to an offshore sourcing arrangement and as such will not be discussed in this Comment.

36. *See* Chen, *supra* note 27, at 7 (asserting that choosing a WFOE model for investment in China is becoming more popular as foreign companies become comfortable with doing business in China, and China becomes comfortable with allowing foreign businesses in); *see also* ZIMMERMAN, *supra* note 25, at 79 (noting that after China's accession to the WTO, U.S. companies have greater flexibility and meet less resistance when setting up WFOEs, leading to the WFOE being the preferred entity of foreign investors).

37. Although there would be contractual obligations between the U.S. subsidiary and its parent, no contract would exist between a U.S. company and a Chinese-owned enterprise because the whole endeavor would be under the complete control of the U.S. company. *See* ZIMMERMAN, *supra* note 25, at 78-81 (discussing the WFOE as being free from outside investment—hence, the "wholly foreign-owned enterprise" label).

38. For each of the arrangements discussed in this section, except for the WFOE arrangement, there will be a contract between the U.S. company and the Chinese counterpart which details the responsibilities of each. *See infra* Part I.B (discussing the substantive contract law of China).

allows the parties to a “foreign-related” contract to choose Chinese law or foreign law as the basis for resolving disputes.³⁹ A foreign-related contract, in the offshore sourcing situation, means that one party is not a Chinese legal person.⁴⁰

China considers the joint venture enterprise that results from the partnership between the U.S. company and the Chinese company a Chinese legal person.⁴¹ While the contract between the U.S. and Chinese companies establishing a joint venture meets the definition of a foreign-related contract, implying choice of law, the Contract Law stipulates that the contracts for Chinese-foreign joint ventures shall apply the laws of China.⁴² Thus, the contract between the U.S. company and the Chinese counterpart that forms the joint venture must choose Chinese law.⁴³ The parties may still choose arbitration as

39. Contract Law (promulgated by National People’s Congress Mar. 15, 1999, effective Oct. 1, 1999), art. 126, *translated at* <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/1> (last visited Aug. 19, 2007) (P.R.C.) [hereinafter Contract Law P.R.C.]. The first clause of Article 126 as translated states:

Parties to a foreign related contract may choose a country’s law as an applicable law for contract dispute resolution unless there is a different provision in any Chinese laws. If parties to a foreign contract fail to choose an applicable law, the laws of the country which has the closest relation to the contract shall be applicable.

WEI LUO, THE CONTRACT LAW OF THE PEOPLE’S REPUBLIC OF CHINA 61 (1999) [hereinafter WEI LUO, CONTRACT LAW P.R.C.]; *see* Mo Zhang, *Choice of Law in Contracts: A Chinese Approach*, 26 NW. J. INT’L L. & BUS. 289, 314-15 (2006) (explaining that the first clause of Article 126 of the Contract Law permits the parties expressly to choose the applicable law for the contract so long as the exception clause is not triggered). The Chinese Contract Law became effective in 1999 and reflects a reform in China to incorporate internationally recognized contract principles such as equality between parties, good faith, and freedom of contract. WEI LUO, CONTRACT LAW P.R.C., *supra*, at 12-13. This reform is a step towards China becoming a more market based economy. *Id.* at 13-14.

40. Mo Zhang, *supra* note 39, at 298 (listing the possible permutations of a foreign contract as “(a) at least one party is not a Chinese citizen or legal person, (b) the subject matter of the contract is in a foreign country (e.g., the item to be sold or purchased is located outside of China), or (c) the conclusion or performance of the contract is made in a foreign country”). Only when a contract is “foreign” under Chinese law does “the question as to which law shall govern the contract become relevant.” *Id.* “If a contract is domestic in nature, it is without question that the contract will be subject to Chinese law only.” *Id.*

41. Regulations for the Implementation of Joint Ventures P.R.C., *supra* note 28, at art. 2. In normal commercial contracts with third parties and joint ventures, the Contract Law P.R.C. would apply. *See* Contract Law P.R.C., *supra* note 39, at art. 126; ZIMMERMAN, *supra* note 25, at 90 nn.46-47. In the United States, joint ventures are part of the state law for corporations. 1 JAMES D. COX & THOMAS LEE HAZEN, COX & HAZEN ON CORPORATIONS § 1.08 (2d ed. 2003). The foreign counterpart of the joint venture is usually considered to be doing business in the state as a partnership and is governed by state law, instead of Chinese law. FLETCHER CYCLOPEDIA *Corporations* § 8500 (1998). However, this Comment does not undertake an analysis of the liability of partnerships in the United States.

42. Contract Law P.R.C., *supra* note 39, at art. 126.

43. *Id.* The second clause of Article 126 states:

the forum for dispute resolution under the Contract Law.⁴⁴ Because the joint venture is a Chinese legal person, the contract and transactions between the China-based provider and the joint venture is a domestic contract and automatically governed by Chinese law.⁴⁵

Similarly, China considers the WFOE a self-contained Chinese legal person upon creation.⁴⁶ For the majority of the transactions the WFOE conducts,⁴⁷ the U.S. company does not have a choice of law or

The laws of the People's Republic of China shall be applied to all Sino-foreign equity joint venture enterprise contracts, Sino-foreign cooperative joint venture enterprise contracts and exploration and development of natural resources contracts which are performed within the territory of the People's Republic of China.

WEI LUO, CONTRACT LAW P.R.C., *supra* note 39, at 61; *see* Mo Zhang, *supra* note 39, at 320 (explaining that although Chinese Contract Law recognizes party autonomy in choosing the law to be applied, the second paragraph of Article 126 has a mandatory exception for Chinese-foreign contractual joint ventures, which must choose Chinese law).

44. Contract Law P.R.C., *supra* note 39, at art. 128. Article 128 states in relevant part:

The parties may resolve a contract dispute[] through settlement or mediation. . . . The parties to a foreign contract may submit their disputes to a Chinese arbitration institution or other arbitration institutions for arbitration according to their arbitration agreement.

WEI LUO, CONTRACT LAW P.R.C., *supra* note 39, at 62.

45. Contract Law P.R.C., *supra* note 39, at art. 126; *see* Mo Zhang, *supra* note 39, at 298 ("If a contract is domestic in nature, it is without question that the contract will be subject to Chinese law only.").

46. Rules for Implementation of WFOEs P.R.C., *supra* note 33, at art. 2 ("Wholly foreign-owned enterprises shall be subject to the jurisdiction of and receive the protection of Chinese laws. Business activities which wholly foreign-owned enterprises engage in within Chinese territory must comply with Chinese laws and regulations and any activity detrimental to China's social public interest shall be prohibited."). Being subject to Chinese law may concern U.S. companies because of the relative lack of transparency and influence of the Chinese Communist Party on the judicial system. Sarah Biddulph, *China's Accession to the WTO: Legal System Transparency and Administrative Reform*, in CHINA AND THE LONG MARCH TO GLOBAL TRADE: THE ACCESSION OF CHINA TO THE WORLD TRADE ORGANIZATION 156 (Sylvia Ostry et al. eds., 2002); Mei Ying Gechlik, *Judicial Reform in China: Lessons from Shanghai*, 19 COLUM. J. ASIAN L. 97, 97-100 (2005). At the same time, a WFOE would theoretically receive the same protection under Chinese law as any other Chinese business because of China's WTO membership. *See* World Trade Organization, Principles of the Trading System, http://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm (last visited Aug. 19, 2007) (describing the principle of national treatment). Interestingly, the United States would consider the Chinese subsidiary of a U.S. company subject to U.S. law for certain purposes. *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 414 (1987) ("[A] state may exercise jurisdiction to prescribe for limited purposes with respect to activities of foreign branches of corporations organized under its laws."); 36 AM. JUR. 2D *Foreign Corporations* § 448 (explaining that by virtue of the minimum contacts doctrine, a subsidiary may be subject to in personam jurisdiction in the state in which its parent is located).

47. Some interactions between the WFOE as a subsidiary to a U.S. company may be governed by U.S. law. "[A] state may exercise jurisdiction to prescribe for limited purposes with respect to activities of foreign branches of corporations organized under its laws." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 414; 36 AM. JUR. 2D *Foreign Corporations* § 448.

choice of forum as between Chinese law and U.S. law with this arrangement.⁴⁸ Chinese law will govern most business the WFOE conducts in China. However, in China, every company must provide an employment contract with its employees.⁴⁹ If the U.S. parent company, not the WFOE, is employing the Chinese programmer, the employment contract is a foreign-related contract and the U.S. company may choose the law and the forum to be applied to that contract.⁵⁰

While the Chinese Contract Law provides some flexibility for U.S. companies sourcing in China, choice of law and choice of forum are voluntary between the parties and relies on the parties including sufficiently clear terms. If protective terms are not included or are not clear, the contracts will not sufficiently protect the U.S. company or U.S. citizens. Thus, the scope of regulatory regimes around offshore sourcing embedded software to China are important to examine to determine legal sources, apart from private contracts, available to protect the United States from malicious code.

II. CHINESE AND U.S. REGULATORY LAW ARE INSUFFICIENT TO PROVIDE PROTECTION TO U.S. CITIZENS AND COMPANIES

China allows foreign companies to invest in China and export high technology goods, subject to some restrictions concerning State

48. Rules for Implementation of WFOEs P.R.C., *supra* note 33, at art. 2.

49. Regulations on the Labor Management of the Foreign-Funded Enterprise (promulgated by Ministry of Labor and Ministry of Foreign Trade & Economic Cooperation, Aug. 11, 1994, effective Aug. 11, 1994), art. 4, 8 (P.R.C.), *translated at* <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/1> (last visited Aug. 19, 2007) [hereinafter Foreign Enterprise Labor Management P.R.C.] (stating that the labor contracts are between the employee and the foreign company and indicating that a foreign funded enterprise must follow the Labour Law); Labour Law of the People's Republic of China (effective Jan. 1 1995), art. 16 (P.R.C.), *translated at* <http://english.mofcom.gov.cn/aarticle/policyrelease/internationalpolicy/200703/20070304475283.html> (requiring a labor contract for any labor relationship). In addition, a foreign-invested enterprise may employ U.S. citizens but must give hiring preference to Chinese nationals. Regulations on the Management of Employment of Foreigners in China (promulgated by Ministry of Labor, Jan. 22, 1996, effective May 1, 1996), ch. 2, arts. 5-6, *translated at* <http://english.mofcom.gov.cn/static/column/lawsdata/chineselaw.html/1> (last visited Aug. 19, 2007) (P.R.C.) [hereinafter Regulations on Employment of Foreigners P.R.C.].

50. Contract Law P.R.C., *supra* note 39, at art. 126. The joint venture arrangement would also have employment contracts with its employees. For those employment contracts to be foreign-related, the contract must be between the U.S. company and the Chinese employee. However, it is also possible in the joint venture that the Chinese partner would hire the Chinese employees and have the employment contract be between the Chinese partner and Chinese employee, making it a domestic contract.

security.⁵¹ Similarly, the United States Congress only minimally regulates offshore sourcing.⁵² Thus, unless the offshore sourcing arrangement is seen as posing a threat to national security, neither Chinese nor U.S. regulatory law will restrict offshore sourcing.

A. *Chinese Law Does Not Restrict Exporting Products Containing Embedded Software*

China promulgated the Foreign Trade Law in 2004 to support its “opening to the outside world” by permitting more freedom to import, export, and invest while ensuring the Chinese government still maintains some oversight.⁵³ Currently, this law does not restrict embedded software production or export.⁵⁴

51. See Foreign Trade Law (promulgated by Nat'l People's Congress, Apr. 6, 2004, effective July 1, 2004), arts. 1, 3, 11, 14, translated at http://www.tdctrade.com/report/reg/reg_040503.htm?w_sid=194&w_pid=703&w_nid=&w_cid=&w_idt=1900-01-01&w_oid=180&w_jid= (P.R.C.) [hereinafter Foreign Trade Law P.R.C.].

52. John F. Delaney, *Privacy, Data Security and Outsourcing: The Regulatory Framework*, in DELANEY & TANENBAUM, *supra* note 8, at 611-34. Often, federal and state regulations are targeted at protecting data that is transferred between business units or companies, such as the Gramm-Leach-Bliley Act of 1999 and the Amendment to California Civil Code Section 1798.82 (requiring businesses that suffer a breach of data security to notify California residents). *Id.* at 632. While there are frequent proposals in state and federal legislatures to limit offshore sourcing, many of these proposals seem to target only government contractors. See, e.g., Gregory B. Hladky, *Blumenthal Pushes Firms with U.S. Workers*, NEW HAVEN REGISTER (Conn.), Feb. 13, 2007, available at http://www.nhregister.com/site/index.cfm?newsid=17843249&BRD=1281&PAG=461&dept_id=517515&rft=8 (reporting that the Connecticut Attorney General proposed legislation giving preference to U.S. companies that do not outsource for state contracts); Chris Seper, *Offshoring Finds Foes in Ohio Legislature*, PLAIN DEALER (Ohio), Apr. 19, 2004, at E4 (reporting on a proposal from lawmakers restricting state and local contracts to companies that do not send work overseas).

53. Foreign Trade Law P.R.C., *supra* note 51, at arts. 1, 3, 11, 14. The Law defines foreign trade as “the import and export of goods, technology, and the international trade of services.” *Id.* art. 2. It also allows the State Council to take action quickly if any import or export situation abruptly or abnormally interferes with the economic security of the state:

The authority responsible for foreign trade under the State Council and other related authorities under the State Council shall develop a surveillance mechanism to deal with emergencies related to import and export of goods and technology and international trade in services, to cope with emergent and abnormal circumstances in foreign trade, and safeguard the country's economic security.

Id. art. 49. Unlike Exon-Florio and section 232, any violation of the Chinese Foreign Trade Law can result in fines or criminal prosecution. *Id.* arts. 60-66. The Foreign Trade Law also implements some of China's obligations under the WTO, granting most favored nation and national treatment to businesses from the United States. *Id.* art. 6. See generally Biddulph, *supra* note 46, at 163-65 (listing examples of China's requirements under the General Agreement on Tariffs and Trade (“GATT”).) So long as the business registers its contracts, and unless another law restricts the imports or exports, the Foreign Trade Law allows the free import and export of goods and services. Foreign Trade Law P.R.C., *supra* note 51, at arts. 14-16. A government circular sets forth procedures to be followed.

To facilitate this trade, the Chinese government provides a catalog that lists products and services which it classifies as encouraged, restricted, or prohibited for export.⁵⁵ China considers products or services not listed to be “permitted” as exports. Significantly, China does not list most goods containing embedded software as restricted or prohibited, making them at least “permitted” as an export.⁵⁶ The catalog lists some products, such as televisions and integrated circuits, which contain embedded software, as encouraged.⁵⁷ Thus, China likely does not restrict a U.S. company from programming embedded software products in China for export back to the United States.

B. U.S. Laws Focus on National Defense

The United States has two main federal laws that could be applied to an offshore sourcing arrangement. First, the Exon-Florio Amendment⁵⁸ to the Omnibus Trade and Competitiveness Act of 1988⁵⁹ authorizes the Committee on Foreign Investment in the United States (“CFIUS”) to investigate acquisitions or mergers with a foreign company and, if necessary, prohibit that acquisition due to

Foreign-funded projects shall be examined and approved, and put on record respectively by the departments of development planning and the economic and trade departments according to the limit of authority for examination and approval; the contracts and articles of association of foreign-funded enterprises shall be examined and approved, and put on record by the departments of foreign trade and economic cooperation.

Circular on Strengthening the Admin. of the Establishment of Sensitive Materials Prod. Enters. in China by Foreign Investors, No. 165 (promulgated by State Dev. Planning Comm., Ministry of Foreign Trade & Econ. Cooperation, State Econ. Comm., May 11, 2002), at 1, *translated at* http://www.fdi.gov.cn/pub/FDI_EN/Laws/InvestmentDirection/GuidanceforSpecificIndustries/P020060620332181098108.pdf (last visited Aug. 19, 2007) (P.R.C.).

54. Catalog of Restricted Foreign Investment Industries (promulgated by State Dev. Planning Comm., Ministry of Foreign Trade & Econ. Cooperation, State Econ. Comm., May 11, 2002, effective May 11, 2002), *translated at* http://www.chinadaily.com.cn/bizchina/2006-04/20/content_572210.htm (P.R.C.) [hereinafter Catalog for Investment P.R.C.]. China does restrict some types of exports “in order to safeguard the national security, public interest, or public ethics.” Foreign Trade Law P.R.C., *supra* note 51, at art. 16. Article 26 of the Foreign Trade Law has the same restriction for international services. *Id.* art. 26.

55. Foreign Trade Law P.R.C., *supra* note 51, at art. 11.

56. *Id.* arts. 4, 11; *see* Catalog for Investment P.R.C., *supra* note 54 (listing the encouraged, restricted, and prohibited export items). China has also issued a Circular specifically addressing questions on software export. Circular Concerning Relevant Questions About Software Exports (promulgated by Ministry of Foreign Trade & Econ. Cooperation et al., Jan. 4, 2001, effective Jan. 4, 2001), *translated at* <http://english.hebiic.gov.cn/policy/PolicyDetail.aspx?id=210> (last visited Aug. 18, 2007) (P.R.C.). This regulation clarifies that unless the software exporting company has a registered capital of more than one million RMB, its exports must be managed by the Ministry of Foreign Trade and Economic Cooperation. *Id.*

57. Catalog for Investment P.R.C., *supra* note 54.

58. 50 U.S.C.A. app. § 2170 (1994).

59. Pub. L. No. 100-418, tit. V, § 5113, 102 Stat. 1432 (1988).

the effect on national security.⁶⁰ Notably for offshore sourcing arrangements, CFIUS may consider a joint venture or “similar arrangement” with a foreign company an acquisition if the foreign company could gain control over the U.S. business.⁶¹

While there may be an instance where an offshore sourcing joint venture arrangement results in the Chinese partner acquiring control of the U.S. company, in typical arrangements, the U.S. company is likely to retain control over most major decisions.⁶² Furthermore, knowing the definition of acquisition under this law, a U.S. company could create the joint venture such that the U.S. company would not lose control over most major decisions.⁶³ As such, it is unlikely that CFIUS would use the Exon-Florio Amendment to prohibit an offshore sourcing arrangement for embedded software, because it would not consider it a possibility that the foreign company could gain control of the joint venture.⁶⁴

Second, the U.S. Trade Expansion Act section 232⁶⁵ allows the President to reduce imports if he determines that the product is being imported “in such quantities or under such circumstances” that threaten U.S. national security.⁶⁶ The Act does not explicitly define

60. *Id.* Note that national security is not defined in the statute. 50 U.S.C.A. app. § 2170; Nance & Wasserman, *supra* note 28, at 951.

61. 31 C.F.R. 800.301 (2006); *accord Alvarez, supra* note 28, at 82-83; Nance & Wasserman, *supra* note 28, at 965-66.

62. *See* Nagel & Murphy, *supra* note 8, at 152 (noting that management’s goal to shed non-core business functions is one reason offshore sourcing is growing, implying that the U.S. company will retain its core functions); *see also* CARMEL & TJIA, *supra* note 8, at 15, 111 (observing that companies tend to keep “creative, innovative, and research oriented” activities in the United States and noting that a “strategic peril” in offshore sourcing is losing the company’s core competency). *See generally* Mendel, *supra* note 8, at 257 (providing the explanation that U.S. companies use offshore sourcing to yield cost savings and increase efficiency, yet the company is “typically able to exert more control” by offshore sourcing to a subsidiary or close foreign affiliate). Moreover, if for some reason the CFIUS did decide to investigate an offshore sourcing joint venture arrangement, the U.S. company could negotiate terms to assure the Committee the requisite level of security, as Lenovo did by moving its headquarters to the United States. Schmertz & Meier, *supra* note 3, at 1. Lenovo Group Ltd., the largest China-based PC maker, acquired IBM’s PC business in 2005. *Id.* The one stipulation for approval was that Lenovo would move its headquarters to the United States from Beijing. *Id.* Today, major production operations are both in China and North Carolina. Michael Schuman, *Lenovo’s Global Gambit*, TIME, Oct. 2006, at G15.

63. *See* Chen, *supra* note 27, at 10 (discussing the control of power in joint ventures and noting that it was not uncommon for the board of directors to create an arrangement that maintains control of the other entity).

64. *See id.* (“The parties to a J[oint] V[enture] will pay particular attention to balancing each partner’s control over the J[oint] V[enture].”).

65. 19 U.S.C. § 1862 (2000).

66. Nance & Wasserman, *supra* note 28, at 929-30. In enacting the section, Congress stated that the purpose was to safeguard the security of the Nation, “not the output or profitability of any plant or industry except as these may be essential to national security.” H.R. REP. NO. 85-1761, at 13-15 (1958).

the term “national security.” Instead, it gives five factors to consider when assessing the level of imports.⁶⁷ These factors indicate that the President should construe national security to mean “national defense.”⁶⁸ Traditionally, the President has implemented restrictions only when there is a threat to national defense.⁶⁹

The past reluctance to use section 232 does not preclude the government from applying it to the embedded software scenario. Because weapons systems are a traditional area of national security,⁷⁰ and because weapons systems contain embedded software,⁷¹ the President could deem importation of weapons systems with embedded software built in China a threat to national security.⁷² However, the same threat of malicious code is present in civilian applications, which are not normally evaluated as a threat to national security.⁷³ Thus, section 232 is inapplicable to many offshore

67. 19 U.S.C. § 1862. The President should consider the following factors: (1) “domestic production of the article needed for projected national defense requirements;” (2) “the capacity of domestic industries to meet such requirements;” (3) “existing and anticipated availabilities of the human resources, products, raw materials, and other supplies and services essential to the national defense;” (4) “the requirements of growth of such industries and such supplies and services, including the investment, exploration, and development necessary to assure such growth;” and (5) “the importation of goods in terms of their quantities, availabilities, character, and use as those affect such industries and the capacity of the United States to meet national security requirements.” 19 U.S.C. § 1862(d). The statute adds that

the Secretary and the President shall further recognize the close relation of the economic welfare of the Nation to our national security, and shall take into consideration the impact of foreign competition on the economic welfare of individual domestic industries; and any substantial unemployment, decrease in revenues of government, loss of skills or investment, or other serious effects resulting from the displacement of any domestic products by excessive imports.

19 U.S.C. § 1862(d). The statute also provides that the Secretary should consider the relationship between economic welfare and national security. 19 U.S.C. § 1862.

68. Nance & Wasserman, *supra* note 28, at 935-36.

69. The investigating authority (the International Trade Administration) specifically considers whether, during a national emergency, the domestic industry can expand production sufficiently, whether the existing stock can be converted from civilian to military use, and whether the imports are reliable. Nance & Wasserman, *supra* note 28, at 938 n.61. The only product that has been unilaterally restricted is petroleum imports from Libya. *Id.* at 945. This restriction is generally viewed as stemming from political considerations rather than the actual stockpile or domestic ability to produce petroleum. *Id.*

70. See Anthes, *supra* note 3 (quoting the opinion of Paul Strassmann, a professor at George Mason University, that a denial of service problem could result in “billion-dollar weapons unable to function”).

71. See, e.g., *id.* (discussing the possible dangers of overseas code in U.S. weapons systems).

72. Nance & Wasserman, *supra* note 28, at 935 (noting the President’s power to determine which imports are a threat to national security).

73. See, e.g., *id.* at 935-36 (explaining that although what is a threat to national security is undefined, “the focus is upon national defense” applications).

sourcing arrangements of embedded software,⁷⁴ requiring a different approach to the embedded software scenario.

III. THE COMPUTER FRAUD AND ABUSE ACT IS A MEANS TO ENHANCE SECURITY

Even though Chinese and U.S. regulatory laws are not likely to reduce the risk of malicious code in the embedded software scenario, the Computer Fraud and Abuse Act (“CFAA”) § 1030 offers a strong remedial tool to counter the scenario.⁷⁵ This act is broad enough to apply in new areas where products use embedded software⁷⁶ and allows for criminal and civil penalties.⁷⁷

74. Cf. Gary G. Yerkey, *U.S. Commerce Department to Publish ‘Catch-All’ Export Rule for China This Spring*, 23 INT’L TRADE REPORTER 427, 433 (2006) (reporting that the Department of Commerce proposed limiting exports from the United States to China that “could damage national security,” for example when the exporter knows the product could have a military end-use).

75. 18 U.S.C. § 1030 (2000). There are also narrower laws that address sabotage of nuclear facilities or airplanes that the United States could use to prosecute a person in those specific situations. See, e.g., 18 U.S.C. § 32 (2000) (providing for fines and imprisonment for the willful damage or disabling of aircraft); 42 U.S.C. § 2284 (2000) (providing criminal penalties for the sabotage of nuclear facilities or fuel). The CFAA can be used in conjunction with these and other specific laws. See, e.g., *United States v. Ivanov*, 175 F. Supp. 2d 367, 370 (D. Conn. 2001) (charging Ivanov with violations of the CFAA, the Hobbs Act, 18 U.S.C. § 1951 (2000), and the Access Device Statute, 18 U.S.C. § 1029 (2000)); *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1258 (N.D. Iowa 2000) (charging National Health Care Discount with a violation of the CFAA and Virginia Computer Crimes Act).

76. See Anthes, *supra* note 3. Anthes references software being used in weapons systems and “systems that bundle the hardware, an operating system, a database and other components in addition to the application code.” *Id.* Many articles, cases, and even the legislative history of the CFAA reference viruses being inserted into the Internet by a “hacker,” or some other act of an outsider using the Internet or a network to obtain information or to impair systems. See, e.g., *Am. Online, Inc.*, 121 F. Supp. 2d at 1272-76 (finding that the defendant violated the CFAA by using the AOL network to send spam e-mail); H.R. REP. NO. 98-894, at 10 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3695-96 (discussing the problem of “hackers” and their proliferation due to the growth of computer networks); Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber—Crime Threat*, 43 AM. CRIM. L. REV. 201, 201-02 (2006) (referencing breaches in security networks regardless of industry); *Spammer, Described as Scourge of In-Box, Is Charged with Fraud*, N.Y. TIMES, June 1, 2007, at A1 (reporting the apprehension of a hacker who used “computers infected with malicious code to send out millions of pieces of spam since 2003”). But see Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 576 (1997) (“[A] ‘computer-specific’ approach results, too often, in criminal statutes that are unnecessary, imprecise, clumsy, over-inclusive, or ineffective.”). What the DOD report and what this Comment attempt to bring to light is the fact that an insider can insert malicious code into any aspect of the broader computing system, without the need of a network. Anthes, *supra* note 3 (“You can put back doors and Trojans in any layer of that environment, not just in the custom code.”). In other words, the malicious code can be inserted when the system is being built.

77. 18 U.S.C. § 1030(c), (g) (establishing fines and imprisonment for violations of subsections (a) and (b) and allowing for a civil action for a violation of clauses (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)). But cf. Reid Skibell, *Cybercrimes and*

U.S. companies can use the CFAA, and its case law interpretations, as a model to incorporate similar language into contracts with Chinese joint venture partners and Chinese employees to provide an additional level of security for the embedded software.⁷⁸ As applied to the embedded software scenario, a U.S. company or the U.S. government can bring a claim in a U.S. court against a Chinese programmer for violating the CFAA.⁷⁹ Because the CFAA can be applied extraterritorially, a U.S. court can validly exercise subject matter jurisdiction over a claim brought against the programmer.⁸⁰

A. *The Computer Fraud and Abuse Act Encompasses Malicious Code in Embedded Software*

For the CFAA to apply substantively to the embedded software scenario, one must first determine if programming malicious code into embedded software violates any sections of the statute. The CFAA prohibits knowingly or intentionally “accessing” a protected computer, “without authorization,” or “exceeding authorized access” of a protected computer, to achieve some additional goal, such as obtaining information or causing damage to the computer.⁸¹ A

Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act, 18 BERKELEY TECH. L.J. 909, 911, 922, 937-39 (2003) (criticizing the overly punitive nature of the CFAA).

78. See *infra* Part III.A.

79. See *infra* Part III.B.

80. See *infra* Part III.C.

81. 18 U.S.C. § 1030. The CFAA states, in relevant part:

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information . . . of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits . . . to any person not entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

...

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer . . . and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ;

(5)

protected computer is a computer used by or for the U.S. government or a computer used in interstate or foreign commerce, even if the computer is physically located outside of the United States.⁸²

-
- (A)
- (i) knowingly causes the transmission of a program, information, code, or command, and . . . intentionally causes damage without authorization, to a protected computer;
 - (ii) intentionally accesses a protected computer without authorization, and . . . recklessly causes damage; or
 - (iii) intentionally accesses a protected computer without authorization, and . . . causes damage; and
- (B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused . . .
- (i) loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value . . . ;
 - . . .
 - (iii) physical injury to any person;
 - (iv) a threat to public health or safety; or
 - (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
- (6) knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—
- (A) such trafficking affects interstate or foreign commerce; or
 - (B) such computer is used by or for the Government of the United States; [or]
- (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;
- shall be punished . . .

18 U.S.C. § 1030(a) (footnote omitted). A violation of the act could be as simple as accessing a protected computer to gain information, so long as the access was an interstate or foreign communication and was intentional. 18 U.S.C. § 1030(a)(2)(C). The act also prohibits accessing a protected computer in order to cause damage to the computer. 18 U.S.C. § 1030(a)(5). The damage caused may be intentional, 18 U.S.C. § 1030(a)(5)(A)(i), reckless, § 1030(a)(5)(A)(ii), or negligent, § 1030(a)(5)(A)(iii). See *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (holding that deleting files from a computer to which the defendant was no longer allowed access, using a secure-erase program which had to be added to the computer, would be violation of the CFAA); *Moulton v. VC3*, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000) (holding that certain methods of scanning a computer to determine security weaknesses do not fit the definition of damage because the scanning did not compromise network security and no information was made unavailable).

82. 18 U.S.C. § 1030(e)(2). A computer includes any “electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *Id.* § 1030(e)(1). Congress then limited the definition by including the clause, “but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.” *Id.* The legislative history suggests that Congress struggled with the definition of computer.

In the embedded software scenario, the embedded software is likely in a device that meets the definition of a protected computer, in part because the software helps the device perform the “logical, arithmetic, or storage functions” needed to meet the definition of computer.⁸³ In addition, the computer is protected by being involved in foreign commerce because the embedded software is programmed into a computer in China, then exported back to the United States.⁸⁴ Thus, applied to the embedded software scenario, the programmer inserts malicious code into a protected computer, as defined by the CFAA.⁸⁵ As a result, the key terms from the statute needing definition are “access” and “authorization.”

The whole issue of defining the word ‘computer’ has plagued the consideration of computer crime legislation since its early days. . . . Initially, it was the Subcommittee on Crime’s opinion that the dictionary definition was as good as one available considering the volatile state of technology in this area. The Committee decided, however, that a specific definition was desirable in order to avoid attacks upon the statute on the grounds of vagueness.

H.R. REP. NO. 98-894, at 23 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3709. Although much of the original 1984 statute has been changed, the definition of “computer” has remained the same since the initial enactment. *Compare* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, tit. II, ch. XXI, 98 Stat. 1837, 2190-92 (1984) (current version at 18 U.S.C. § 1030 (2000)), *with* 18 U.S.C. § 1030(e)(1). A 1979 proposal suggested that the definition be: “an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.” Olivenbaum, *supra* note 76, at 619 n.202 (citation omitted). While Congress recognized the need for “computer-specific” statutes, the pace at which technology changes risks making these statutes inapplicable to certain situations. *Id.* at 576; *accord* President’s Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct on the Internet*, Mar. 2000, <http://www.cybercrime.gov/unlawful.htm#TECH> (recommending that any regulation of unlawful conduct on the Internet should be treated in a technology-neutral manner).

83. *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005) (explaining that the statute is general, likely allowing iPods, wireless base stations, cell phones, cell towers, and other items to be considered computers, and that it is the legislature’s duty, not the courts’, to amend the statute to give it less coverage); Lee, *Embedded Software*, *supra* note 1, at 1 (explaining embedded software to have as its principal role the interaction with the physical world via the device in which it resides, such as a car, airplane, or telephone).

84. *Accord* *Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1291 (3d Cir. 1979) (stating that the Supreme Court classified foreign commerce as applying to “importing, exporting, and other commercial transactions as well as transportation and communication between the United States and a foreign country”); *see* *United States v. Ivanov*, 175 F. Supp. 2d 367, 374 (D. Conn. 2001) (distinguishing foreign commerce and interstate commerce).

85. Note that the end product might not be a “computer,” as commonly thought, but even devices such as CD players contain sufficient software to be considered “micro-computers.” *See* Graaf, *supra* note 1, at 61 (explaining that many devices today contain software).

The statute does not define the term “access,” but accessing a computer is a requirement for liability in all but two of the seven subsections in section 1030(a).⁸⁶ Due to advances in computer technology since Congress wrote the statute, courts interpret the word “access” along a continuum of broad to narrow.⁸⁷

One broad interpretation of “access” is “the freedom or ability to make use of.”⁸⁸ The court in *America Online, Inc. v. National Health Care Discount, Inc.*,⁸⁹ acknowledged that the statute did not define “access”⁹⁰ and consequently turned to Merriam-Webster’s Collegiate Dictionary. According to the dictionary, “access” means “to exercise the freedom or ability to . . . make use of something.”⁹¹ The court

86. 18 U.S.C. § 1030(a). Subsections (1) and (4) prohibit knowingly accessing a protected computer. § 1030(a)(1), (a)(4). Subsections (2), (3), and (5) prohibit intentionally accessing a protected computer. § 1030(a)(2), (a)(3), (a)(5).

87. See generally Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003). Professor Orin Kerr has explored the limitations of not having a definition of access in the statute. *Id.* at 1620-21. In his article, he comments that “access” can have two different meanings—“first, that a user accesses a computer when she sends a command to that computer instructing it to perform a task, and the computer performs the request as instructed” or alternatively, “that a user accesses a computer when she sends a command requesting information and the computer responds by sending back the requested information.” *Id.* Thus, without a definition in the statute it is unclear which of these meanings should be applied by courts because the advance of computer technology since the 1970s makes the definition of access no longer self-explanatory. *Id.* at 1620-21, 1641. Proponents of “unauthorized access” laws see these laws as analogous to the traditional breaking and entering or trespass laws, making the concept of “access” easy to envision. *Id.* at 640-41. Today, however, the question becomes: what is a physical presence when there are “always on” Internet connections? *Id.* at 641. While in 1975 a user had to dial-in to a computer network using a telephone line and usually enter some text-based identification to proceed, today’s users “merge seamlessly” with the Internet and the computers connected to it. *Id.* “[T]oday you might know when you use a computer, but the word ‘access’ is merely a label to be assigned somewhat awkwardly to conduct that may not seem like an access at all.” *Id.*; accord Olivenbaum, *supra* note 76, at 576 (“To the extent that they are drafted in ‘technology-specific’ language, the pace of technological change and the ingenuity of computer-literate criminals guarantee that those statutes will be obsolete almost as soon as they are enacted.”).

88. See *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1272-73 (N.D. Iowa 2000) (citing MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 6 (10th ed. 1994)).

89. 121 F. Supp. 2d 1255. In this civil case, America Online, Inc. (“AOL”) brought suit against National Health Care Discount, Inc. (“NHCD”) for sending unsolicited bulk email, or “spam,” through the AOL network to members’ email. *Id.* at 1259. The contractor for NHCD harvested the AOL members’ email addresses, then sent out hundreds of millions of emails regarding the NHCD products, often using inaccurate “From” information. *Id.* at 1266-67.

90. *Id.* at 1272.

91. *Id.* at 1273 (internal quotation marks omitted). In the context of *America Online, Inc.*, “when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore ‘accessing’ them.” *Id.* at 1273. As such, NHCD made use of the AOL member computers in violation of the CFAA. *Id.* at 1273; see *Role Models Am., Inc. v.*

held that the sender of an email makes use of the computers through which the message travels and, therefore, accesses those computers.⁹² A similar statute in Kansas defined “access” as “to approach . . . or otherwise make use of any resources of a computer.”⁹³ But, in *State v. Allen*,⁹⁴ the Kansas Supreme Court chose to narrow the definition of the state statute using the Webster’s Dictionary definition—“freedom or ability to make use of.”⁹⁵ In *Allen*, the court found that the defendant did not make use of Southwestern Bell’s telephone system simply by viewing the log-in prompt, and thus did not “access” the system.⁹⁶ Since the defendant did not go beyond the log-in prompt or enter a password, he did not have the ability to use the company’s computers, and thus did not access them.⁹⁷

In the embedded software scenario, the programmer physically accesses the software embedded in the computer to modify it or insert malicious code.⁹⁸ The programmer goes beyond merely approaching and viewing a log-in prompt, as in *Allen*. Instead, the programmer alters or adds code to the protected computer. Although in other cases, like *Allen*, it may be unclear whether a defendant has accessed the computer, in the embedded software scenario the programmer actively “exercise[s] the freedom or ability to make use of” the computer to program his or her malicious code.⁹⁹ Under either definition of access, the programmer in the embedded

Jones, 305 F. Supp. 2d 564, 566-67 (D. Md. 2004) (citing *Am. Online, Inc.*, 121 F. Supp. 2d at 1272-73) (observing that “the word ‘access,’ in this context, is an active verb: it means ‘to gain access to,’ or ‘to exercise the freedom or ability to make use of something;’” therefore, passively receiving information is not accessing the computer from which the information came); *State v. Riley*, 846 P.2d 1365, 1367-68, 1373 (Wash. 1993) (en banc) (holding that Riley accessed the telephone company’s computers without authorization by repeatedly dialing the access number for long distance calls and guessing random passwords in an attempt to learn which passwords would allow him to make long distance calls and charge the calls to another telephone company customer).

92. *Am. Online, Inc.*, 121 F. Supp. 2d at 1272-73.

93. KAN. STAT. ANN. § 21-3755(a)(1) (1996) (amended in 1997 to strike the word “approach” from the definition of “Access”). Since the Kansas statute is similarly worded to the federal CFAA, it is relevant to use as an analogy.

94. 917 P.2d 848 (Kan. 1996).

95. *Id.* at 852-53 (explaining that the wording “to approach” in the statutory definition lent itself to too broad an application).

96. *Id.* at 853; see Kerr, *supra* note 87, at 1624, 1646-47 (describing *Allen* and commenting that courts should interpret “access” even more broadly than the *Allen* court did, while narrowing the interpretation of “unauthorized”).

97. *Allen*, 917 P.2d at 853. Otherwise, under the definition in the state statute, “any unauthorized physical proximity to a computer could constitute a crime.” *Id.* at 852 (citation omitted).

98. 18 U.S.C. § 1030(e) (2000).

99. See *Am. Online, Inc. v. Nat’l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1272-73 (N.D. Iowa 2000) (defining “access” as an active verb “to exercise the freedom or ability to make use of something”).

software scenario accesses the protected computer to insert the malicious code.

To violate the CFAA, the Chinese programmer must also either “exceed authorization” to access the protected computer or access the protected computer “without authorization.” The first case interpreting access without authorization was *United States v. Morris*,¹⁰⁰ which established the “intended function” test.¹⁰¹ Morris, a student at Cornell with authorized access to the Cornell computer system, released a computer virus into the Internet.¹⁰² The court held that individuals with some access to a protected computer can still be without authorization.¹⁰³ Specifically in that case, although Morris had access to a function of the Cornell computer system, he did not use the features of the computer “in any way related to their intended function,” which made the use unauthorized.¹⁰⁴ Similarly, in the embedded software scenario, the programmer has authorized access to the original code, but by adding code in such a way that the original code does not perform its intended function, the

100. 928 F.2d 504 (2d Cir. 1991).

101. *Id.* at 510. Although the case was decided under the 1988 version of the CFAA, it is still relevant. The key terms in the 1988 version are carried over to the current statute. Compare 18 U.S.C. § 1030(a)(5)(A)(iii) (2000) (“intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage”), with 18 U.S.C.A. § 1030(a)(5) (1986) (“intentionally accesses a Federal interest computer without authorization, and . . . damages, or destroys information in any such Federal interest computer”).

102. 928 F.2d at 505, 509. “Morris was authorized to use computers at Cornell As a result, Morris was authorized to communicate with other computers on the network to send electronic mail” *Id.* at 509. Morris argued that the release of the virus via the Cornell computer only “exceed[ed] authorized access” and thus did not violate § 1030(a)(5)(A). *Id.* at 510. Morris relied on a Senate report that stated the statute was aimed at outsiders who would not have access to Federal interest computers. *Id.* Interestingly, Morris claimed to have released the virus only to expose weaknesses in the Internet. *Id.* at 505.

103. See *id.* at 510 (countering that the Senate report also included as an outsider any person who is outside of his or her government department, even though he or she may be a government employee).

104. *Id.* at 510. As Professor Kerr notes, the court may have been drawing on a seemingly unspoken rule in the computer world. Kerr, *supra* note 87, at 1632 (“Although the court did not elaborate on its standard, the intended function test appears to derive largely from a sense of social norms in the community of computer users.”). A software program is designed and built to perform certain tasks, “and network providers enable the programs to allow users to perform those tasks.” *Id.* at 1632. However, by providing the program, the provider “implicitly authorizes users to use their computers to perform the intended functions, but implicitly do not authorize users to exploit weaknesses in the programs that allow them to perform unintended functions.” *Id.* “When a user exploits weaknesses in a program and uses a function in an unintended way to access a computer, the thinking goes, that access is ‘without authorization.’” *Id.*

programmer accesses the software, and thus the computer, without authorization.¹⁰⁵

Notably, the Senate detailed its intention to distinguish between “insiders” and “outsiders” in a 1986 Report regarding the CFAA.¹⁰⁶ The Report stated that Congress did not intend the statute to punish “insiders” who legitimately had access to a government computer but who had exceeded this access in the course of their employment.¹⁰⁷ The Report attempted to make clear that Congress authorized these “insiders.”¹⁰⁸ Arguably then, for the embedded software scenario, the programmer merely “exceeds authorized access” because the programmer is an “insider” in the company; the programmer has authorized access to the protected computer to develop the embedded software as part of his or her job.¹⁰⁹ This means that the programmer did not violate CFAA sections (a)(3) nor (a)(5), which require the access of the protected computer to be “without authorization.”¹¹⁰

The programmer, however, could violate CFAA sections (a)(2)(C) or (a)(4), which prohibit exceeding authorization to obtain information from any protected computer involved in interstate or foreign commerce or using such computer to further a fraud.¹¹¹ For example, the court in *EF Cultural Travel BV v. Explorica, Inc.*¹¹² found

105. *Contra* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000) (discussing the definition of “without authorization” and wondering if, by violating the Terms of Service, the user’s access then becomes unauthorized for purposes of the statute). AOL members have authorization to access the AOL network by virtue of being members, but the AOL Terms of Service specifically state that members are not permitted to send spam e-mail. *Id.* at 1260. The court held that, ultimately, authorization is a question of fact, but used the “insider” versus “outsider” metaphor Congress used when forming the statute. *Id.* at 1273. (“Similarly, is the member converted from an ‘insider’ to an ‘outsider’ for purposes of the CFAA by violating AOL’s policies? On the other hand, if AOL members are ‘outsiders,’ then why would AOL’s membership policies apply to them at all?”).

106. S. REP. NO. 99-432, at 7-8 (1986), as reprinted in 1986 U.S.C.C.A.N. 2479, 2485-86.

107. *Id.* The Senate thought this “exceeding [of] authorization” could be handled via administrative disciplinary procedures. *Id.* Additionally, the Senate was concerned that people authorized to repair the computers, which includes altering data, would be charged or sued under the Act. *Id.* at 12.

108. *Id.*

109. This flows logically from the embedded software scenario. As explained, the programmer’s job is to access the software to program it. The programmer, however, exceeds this authorized access as soon as he or she attempts to maliciously add or change the software.

110. 18 U.S.C. § 1030(a)(3), (a)(5) (2000).

111. 18 U.S.C. § 1030(a)(2)(c), (a)(4).

112. 274 F.3d 577 (1st Cir. 2001). This case involved the defendant, Explorica, using a “scraper program” to gather information from EF’s website on pricing packages of tours for high school students. *Id.* at 579. A scraper program is like a robot that gathers information quickly from the Internet. *Id.* The defendants

that a former employee exceeded authorized access of EF's website because the access went beyond the terms of a confidentiality contract by obtaining proprietary information.¹¹³ A programmer in the embedded software scenario could program malicious code to record a user's personal information then use that information to gain access to personal accounts, thereby obtaining information in violation of (a)(2)(C) and furthering a fraud in violation of (a)(4).

This reasoning is useful, as it relates to the embedded software scenario, particularly if the U.S. company incorporates scope of access provisions into the contract with the Chinese provider and employees. The U.S. plaintiff can argue that access to the software beyond what the parties stipulated in the contract "exceeds authorization," and thus violates the CFAA, so long as the Chinese programmer obtains some information or furthers a fraud.¹¹⁴

While the "insider" versus "outsider" distinction could present a challenge to charging the Chinese programmer under the sections that require access without authorization, a properly constructed contract can help the government charge a person under the sections that allow for "exceeding authorization."¹¹⁵ On the other hand, using the *Morris* "intended function" test, the programmer goes beyond merely "exceeding authorized access" and into "without authorization" because programming malicious code into the computer is not using the computer "in any way related to [its] intended function."¹¹⁶ Thus, it is "without authorization" under all sections of the CFAA regardless of whether the programmer is considered an "insider" or "outsider."¹¹⁷

created this scraper program specifically to gather tour information from EF's website in order to undercut their prices. *Id.* Explorica's vice president, as a former employee of EF, knew what type of information Explorica would need to create the scraper program. *Id.* When the vice president left EF, he signed a confidentiality contract stating that he would not use any business information contrary to the interests of EF. *Id.* at 582.

113. *Id.* at 583-84. Note that although § 1030(a)(4) requires an intent to defraud, the court did not rule on this intent because it was not raised in the briefs. *Id.* at 581 n.9. Thus, the court solely ruled on whether using the scraper program went beyond the terms of the confidentiality agreement and in turn exceeded authorization. *Id.* at 581-84.

114. *See, e.g., id.* (discussing the way that a contract can determine what actions "exceed authorization").

115. 18 U.S.C. § 1030(a)(1), (a)(2), (a)(4). Importantly, the subsection under which a U.S. company may bring a private right of action requires that the access be "without authorization," not merely exceeding authorization. 18 U.S.C. § 1030(a)(5).

116. *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991).

117. 18 U.S.C. § 1030. The United States could take a lesson from China in this matter. The Chinese Criminal Code's broad statement that the government may punish any interference in the normal functioning of a computer information system

B. The U.S. Company Should Choose U.S. Law or Incorporate the CFAA Language into Private Contracts

For the U.S. company in the embedded software scenario to ensure it can benefit from the private right of action in the CFAA, the company must explicitly choose U.S. law as the governing law in any foreign-related contract.¹¹⁸ In addition, the company should choose the United States or arbitration as the forum.¹¹⁹

Even if the contract is governed by Chinese law, the parties can use the CFAA as a guide to incorporate provisions to increase the security of the embedded software.¹²⁰ For example, the contract should state that programming malicious code into the embedded software constitutes unauthorized access. Any breach of these provisions would be a breach of contract, even under Chinese Contract Law.¹²¹

Because China recognizes the freedom of parties to contract and state their own terms, it is possible that the parties may not include such protective language or may not choose U.S. law in a foreign-related contract. Even so, a U.S. company or the U.S. government can still pursue a CFAA claim in a U.S. court against the Chinese programmer, as discussed below.

C. Using the Extraterritoriality of the CFAA to Enforce Security in Offshore Sourcing Situations

If a U.S. company or the U.S. government brings a claim against the Chinese programmer who is part of the embedded software scenario, a U.S. court can find subject matter jurisdiction over the CFAA claim, regardless of whether the U.S. company was able to

covers more instances of embedded software by focusing on the result, rather than the definition of “computer” or “access without authorization.” WEI LUO, THE 1997 CRIMINAL CODE OF THE PEOPLE’S REPUBLIC OF CHINA: WITH ENGLISH TRANSLATION AND INTRODUCTION 156 (Hein & Co. 1998) [hereinafter WEI LUO, 1997 CRIMINAL CODE] (stating art. 286). According to the Chinese Criminal Code, if the normal functioning of what, at the time, is considered a computer is impaired, then the person has violated the law. *Id.*

118. See *supra* Part I.B (discussing choice of law and choice of forum in offshore sourcing arrangements). The foreign-related contracts in the embedded software scenario are primarily the employment contracts between the U.S. company and Chinese programmers. The contract that produces the joint venture must be governed by Chinese law. See *id.*; see also *supra* note 49 and accompanying text (explaining that all employers must have employment contracts with their employees).

119. See *supra* Part I.B.

120. See, e.g., *Morris*, 928 F.2d at 510 (explaining how contracts can provide broad protection, even when the actions taken do not fit within the requirements of the statute).

121. Contract Law P.R.C., *supra* note 39, at art. 8.

choose U.S. law through a foreign-related contract.¹²² In this situation, to have subject matter jurisdiction, the court must be able to apply the CFAA extraterritorially because the Chinese programmer is located in China and much of the conduct began in China.¹²³

Before a court can apply the CFAA to prosecute the Chinese programmer, the U.S. plaintiff must overcome the presumption against extraterritoriality.¹²⁴ Stated in 1909 in *American Banana Co. v. United Fruit Co.*,¹²⁵ the presumption against extraterritoriality requires the court to presume that a statute only applies within the United States.¹²⁶ Even language such as “every person” and “every contract” will be read as meaning only everyone within the territory for which Congress has the constitutional authority to legislate, which is usually the United States.¹²⁷

There are, however, three ways to overcome the presumption against extraterritoriality and find subject matter jurisdiction. First, the language and legislative history of the statute can be evidence of Congress’s intent for the statute to be applied extraterritorially.¹²⁸ Second, even if the statute is silent or ambiguous on its intent, if

122. The U.S. company can claim that the Chinese programmer violated the CFAA. 18 U.S.C. § 1030 (a) (5) (B). 18 U.S.C. § 1030 (g) states, in part, “A civil action for a violation of this section may be brought only if the conduct involves one of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a) (5) (B).” The U.S. government may also file a criminal case against the Chinese programmer for violating any section of the CFAA. § 1030 (c).

123. There are many ways a court could have jurisdiction over the Chinese programmer. For the embedded software scenario in this Comment, personal jurisdiction is not likely a viable method for the court because the scenario assumes the Chinese programmer is not physically in the United States and likely has no minimum contacts with the United States. *See, e.g., Burnham v. Superior Court*, 495 U.S. 604, 619 (1990) (“[J]urisdiction based on physical presence alone constitutes due process because it is one of the continuing traditions of our legal system that define the due process standard of ‘traditional notions of fair play and substantial justice.’”). As the Supreme Court held in the landmark jurisdiction case of *International Shoe Co. v. Washington*:

[D]ue process requires only that in order to subject a defendant to a judgment *in personam*, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice. 326 U.S. 310, 316 (1945). If either of these is true, then the court may have personal jurisdiction. A court may also have diversity jurisdiction because the programmer is Chinese and the business or government is American, but the amount in controversy must be more than \$75,000. 28 U.S.C. § 1332 (2000). This Comment focuses on extending the CFAA extraterritorially, and finding federal question subject matter jurisdiction for a claim brought against a programmer in China under this statute.

124. *Am. Banana Co. v. United Fruit Co.*, 213 U.S. 347, 357 (1909) (discussing the presumption against extraterritoriality).

125. *Id.*

126. *See id.* at 357 (“All legislation is prima facie territorial.”).

127. *Id.*

128. *See infra* Part III.C.1 (analyzing the application of statutory interpretation to the CFAA and the embedded software scenario).

there is a substantial and intentional harmful effect within the territory of the United States, then the court can find jurisdiction.¹²⁹ Finally, if there was significant conduct within the territory of the United States that was essential to the crime or fraud, then the court can find jurisdiction, even if the statute is silent.¹³⁰ Unless the plaintiff satisfies one of these conditions, the court cannot assume “an intent to punish all whom [it] can catch.”¹³¹

While courts have consistently applied “market statute” claims—such as antitrust and securities fraud claims—extraterritorially,¹³² a brief opinion, *United States v. Ivanov*¹³³ was the first case to apply the CFAA extraterritorially. Even though the CFAA is not a traditional economic law statute, the district court properly extended the law extraterritorially in *Ivanov* using similar reasoning to that in the antitrust and securities cases.¹³⁴ As such, U.S. courts can and should

129. See *infra* Part III.C.2 (analyzing the application of the effects test as developed from antitrust case law to the CFAA).

130. See *infra* Part III.C.3 (analyzing the application of the conduct test as developed from securities case law to the CFAA).

131. *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443 (2d Cir. 1945). There is a difference between the jurisdiction to prescribe and the jurisdiction to adjudicate. A court or legislature may have jurisdiction to prescribe or apply a law extraterritorially if it satisfies one of these principles, but it may not be able to enforce that law against a non-citizen if that person is not within the territory of the United States. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 421 cmt. a (1987). Generally, U.S. law requires an extradition treaty with the non-citizen’s country in order to try that person in the United States for crimes committed abroad. 18 U.S.C. § 3181(a) (2000) (“The provisions of this chapter relating to the surrender of persons who have committed crimes in foreign countries shall continue in force only during the existence of any treaty of extradition with such foreign government.”). As yet, the United States does not have an extradition treaty with China, although the two countries do have a Mutual Legal Assistance Treaty. Mutual Legal Assistance in Criminal Matters, June 19, 2000, U.S.-P.R.C., Temp. State Dept. No. 01-44. However, this Comment takes the approach that, similar to the application of the antitrust statutes and the fraud provisions of the securities statutes, a court could still adjudicate a CFAA claim against a Chinese programmer, regardless of the existence of an extradition treaty. See, e.g., *United States v. Nippon Paper Indus. Co.*, 109 F.3d 1, 4-5, 9 (1st Cir. 1997) (holding that acts committed abroad but having effects in the United States may be a basis for criminal prosecution under the Sherman Act). See generally Charles J. Johnson, Jr., *Application of Federal Securities Laws to International Securities Transactions*, 45 ALB. L. REV. 890, 891-92 (1981) (summarizing that courts apply the antifraud provisions of the 1934 Securities Act extraterritorially, while perhaps courts are more restrained in applying the registration rules for securities extraterritorially).

132. Accord Roger P. Alford, *The Extraterritorial Application of Antitrust Laws: The United States and European Community Approaches*, 33 VA. J. INT’L L. 1, 7-19 (1992) [hereinafter Alford, *Extraterritorial Antitrust Laws*] (reviewing the antitrust case law where courts have applied the Sherman Act extraterritorially); John W. Hamlin, Comment, *Exporting United States Law: Transnational Securities Fraud and Section 10(b) of the Securities Exchange Act of 1934*, 3 CONN. J. INT’L L. 373, 385-96 (1988) (reviewing the securities case law where courts have applied section 10(b) of the 1934 Securities Act extraterritorially).

133. 175 F. Supp. 2d 367 (D. Conn. 2001).

134. *Id.* at 370, 373-75.

continue to apply the CFAA extraterritorially in embedded software scenario cases.

1. *The CFAA statutory language and legislative history show intent for its extraterritorial application*

One method of overcoming the presumption against extraterritoriality for the CFAA is to interpret its language and history.¹³⁵ The statutory language does not have to be explicit in stating that a court can apply the statute extraterritorially; the language may simply reference that the statute includes foreign commerce.¹³⁶ In addition, if the legislative history indicates that Congress intended the statute to reach beyond the territorial bounds of the United States to protect U.S. citizens, then a court can find jurisdiction.¹³⁷

A court will first examine the plain language of the statute for clues from Congress as to whether it intended the statute to apply extraterritorially. The court in *Kauther SDN BHD v. Sternberg*¹³⁸ began with this plain language interpretation for section 10(b) of the 1934 Securities and Exchange Act (“1934 Securities Act”).¹³⁹ The court

135. *See id.* at 373 (“[T]his ‘presumption against extraterritoriality’ may be overcome by showing ‘clear evidence of congressional intent to apply a statute beyond our borders.’” (citation omitted)).

136. *E.g.*, *Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 664-65 (7th Cir. 1998) (suggesting that because Section 10(b) of the 1934 Securities and Exchange Act defines “interstate commerce” in part as trade between any foreign country and any State, that Congress would have wanted the Section to be applied extraterritorially).

137. *See id.* at 663-64 (positing that if the legislative history of the 1934 Securities and Exchange Act had given the court any direction, the court would have used that history to help determine extraterritoriality); *SEC v. Kasser*, 548 F.2d 109, 116 (3d Cir. 1977) (holding that Congress’s purpose, for both the 1933 and 1934 Securities Acts, was to ensure high standards for investments in the United States, even for investors from abroad).

138. 149 F.3d 659 (7th Cir. 1998).

139. *Id.* at 664. *But cf.* *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443-44 (2d Cir. 1945) (assuming that the Sherman Act does not cover agreements unless an effect within the United States could actually be shown, without discussing the exact language of the Sherman Act). Section 10(b) of the 1934 Securities and Exchange Act states that

[i]t shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j(b) (2000). The SEC then promulgated Rule 10b-5, which states that [i]t shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

noted that section 10(b) prohibits fraud via “interstate commerce or of the mails in connection with the purchase or sale of any security.”¹⁴⁰ The 1934 Securities Act defines “interstate commerce” to include “trade, commerce, transportation, or communication . . . between any foreign country and any State.”¹⁴¹ While the statute does not explicitly state that courts can apply it extraterritorially, the court held that because the definition of interstate commerce included trade with foreign countries, it showed Congress’s intention for the Act to be applied as such.¹⁴²

The 1934 Securities Act applied extraterritorially in part because it included the key words “commerce . . . between any foreign country and any State.”¹⁴³ The court in *Ivanov* used similar language from the CFAA to extend the CFAA extraterritorially.¹⁴⁴ The district court in *Ivanov* specifically held that, for the CFAA, the government overcame the presumption against extraterritoriality because the CFAA uses the key terms “interstate or foreign commerce or communication,” to apply to computers.¹⁴⁵ By using both the words “interstate” and “foreign”, Congress intended the CFAA to apply both within the United States and abroad.¹⁴⁶ Consequently, the court found the language of the CFAA sufficient to overcome the presumption against extraterritoriality.¹⁴⁷

Despite the fact that the court in *Kauther* did not find explicit legislative history to support its interpretation that it could apply the

-
- (a) To employ any device, scheme, or artifice to defraud,
 - (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
 - (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b-5 (2007).

140. *Kauther*, 149 F.3d at 664 (7th Cir. 1998); see 15 U.S.C. § 78j(b) (“It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails . . . [t]o use or employ . . . any manipulative or deceptive device . . .”).

141. 15 U.S.C. § 78c(a)(17) (2000); *Kauther*, 149 F.3d at 664.

142. *Kauther*, 149 F.3d at 664 (“Congress did leave some indication in the language of the securities laws about their intended application to foreign commerce.”).

143. *Id.*; see *Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1291 (3d Cir. 1979) (defining foreign commerce as “importing, exporting, and other commercial transactions, as well as transportation and communication between the United States and a foreign country”).

144. 175 F. Supp. 2d 367, 374 (D. Conn. 2001).

145. *Id.*

146. *Id.*

147. *Id.*

1934 Securities Act extraterritorially, the *Ivanov* court found support in the 1996 Senate Report regarding the CFAA.¹⁴⁸ Congress added language to protect computers used in foreign commerce to the CFAA in 1996.¹⁴⁹ In its Report, Congress stated its concern that before 1996 the CFAA did not protect computers used in foreign commerce even though “hackers are often foreign-based.”¹⁵⁰

In the embedded software scenario, a court should find subject matter jurisdiction over a CFAA claim against the Chinese programmer using reasoning identical to that in *Ivanov*, supported by *Kauther*.¹⁵¹ Congress must have intended the statute to apply extraterritorially because the CFAA contains language that references both interstate and international commerce.¹⁵² Furthermore, Congress added the 1996 CFAA amendments to address the scenario where a person not located in the United States exceeds authorization or accesses without authorization a computer used in foreign commerce yet located in the United States.¹⁵³ Likewise, in the embedded software scenario, the Chinese programmer is not located in the United States and at least exceeds authorized access of a protected computer located within the United States. As a result, a court can exercise subject matter jurisdiction for a CFAA claim brought against the Chinese programmer.

2. *The effects test allows a court to extend the CFAA extraterritorially*

Even if the statutory language and history is silent or ambiguous, a court can use the effects test to determine extraterritorial application of the CFAA.¹⁵⁴ The effects test, also called the objective territorial

148. *Id.*

149. S. REP. NO. 104-357, at 3 (1996).

150. *Ivanov*, 175 F. Supp. 2d at 374; S. REP. NO. 104-357, at 4.

151. See *Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 664 (7th Cir. 1998) (noting that courts have concluded the statutory language indicates that the antifraud provisions are applicable to at least some securities transactions); *Ivanov*, 175 F. Supp. 2d at 374-75 (arguing that Congress’s intent is clear in that it wanted the CFAA to apply to “computers used ‘in interstate or foreign commerce or communication’”).

152. See, e.g., 18 U.S.C. § 1030(a)(2)(C) (2000).

153. See *Ivanov*, 175 F. Supp. 2d at 374 (citing the 1996 Senate Report to suggest that Congress was concerned about the threat of foreign-based hackers); S. REP. NO. 104-357, at 3-5 (1996). The person would also have to meet one of the additional requirements in any of the seven sections of § 1030(a) in order to be charged. See *supra* note 81 (listing the specific requirements of the CFAA).

154. A court can use this test in conjunction with the statute’s language and history or as an individual test. See, e.g., *Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1291-92 (3d Cir. 1979) (conceding that other courts have found the Sherman Act language not to prohibit extraterritorial application, and primarily using the effects test to find jurisdiction); *Ivanov*, 175 F. Supp. 2d at 370-74 (using both the effects test and statutory interpretation to apply the CFAA extraterritorially).

principle, asserts the U.S. interest in punishing acts that have a detrimental effect within the United States but occur outside its boundaries.¹⁵⁵

Under the effects test, a country may hold a person liable under its laws “for conduct outside its borders that has consequences within its borders which the [country] reprehends”¹⁵⁶ The conduct in other countries must have caused “foreseeable and substantial harm” to interests in the United States for a U.S. court to find jurisdiction.¹⁵⁷ In addition, the effects on the United States must be actual effects.¹⁵⁸ An unparticularized harmful effect in the United States is not enough to justify extending a statute extraterritorially.¹⁵⁹ Furthermore, if the defendant did not intend to cause harm within the United States, then a court cannot find subject matter jurisdiction.¹⁶⁰

One of the first cases to use the effects test was a market access case—*United States v. Aluminum Co. of America* (“*Alcoa*”)¹⁶¹—in 1945.¹⁶² In *Alcoa*, an antitrust case, the court held that, despite the presumption against extraterritoriality, it was also settled law that the United States may hold liable any person for acts done in another country but which have effects within the United States.¹⁶³ *Alcoa*, a Pennsylvania aluminum company with many subsidiaries, had allegedly agreed with foreign aluminum manufacturers to limit its imports into the foreign countries, while the foreign companies agreed either not to import into the United States or to do so under

155. Alford, *Extraterritorial Antitrust Laws*, *supra* note 132, at 4 (defining the effects test as the ability of a state to assert jurisdiction “over conduct outside its borders where such conduct has the intended effect of causing a substantial adverse impact within the state’s territory” and noting that it is the exercise of jurisdiction under this test that has produced the most conflict among nations); Hamlin, *supra* note 132, at 379 (using the term “objective principle” to refer to the effects test). *See generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402(1)(c), § 402 cmt. d (1987) (summarizing a state’s jurisdiction to prescribe law when “conduct outside its territory has or is intended to have substantial effect within its territory” as an aspect of the territoriality principle, but qualifying that it should be only when reasonable under § 403).

156. *Timberlane Lumber Co. v. Bank of Am., N.T. & S.A.*, 549 F.2d 597, 610 (9th Cir. 1976); *United States v. Aluminum Co. of Am. (Alcoa)*, 148 F.2d 416, 443 (2d Cir. 1945). *See generally* ANDREAS F. LOWENFELD, *INTERNATIONAL ECONOMIC LAW* 346-47 (2002) (tracing briefly the history of the effects test through the antitrust case law).

157. *Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 665 (7th Cir. 1998); *Mannington Mills*, 595 F.2d at 1296 n.6.

158. *Alcoa*, 148 F.2d at 444.

159. *Int’l Inv. Trust v. Cornfeld*, 619 F.2d 909, 917 (2d Cir. 1980); *Bersch v. Drexel Firestone, Inc.*, 519 F.2d 974, 989 (2d Cir. 1975).

160. *Bersch*, 519 F.2d at 989.

161. 148 F.2d 416 (2d Cir. 1945).

162. *Id.* at 421 (referring to the Aluminum Company of America as “*Alcoa*, that being the name by which the company has become almost universally known”).

163. *Id.* at 443.

fixed amounts.¹⁶⁴ The court stated that although the cartel made the agreement outside the United States, it equaled an agreement to fix prices, violating the Sherman Act.¹⁶⁵ The effects test was satisfied because the agreement intended to restrict aluminum imports and exports, and the agreement actually restricted aluminum imports and exports.¹⁶⁶

U.S. courts continued to apply the effects test after *Alcoa*, notably in antitrust cases,¹⁶⁷ including in 1979 in *Mannington Mills, Inc. v. Congoleum Corp.*¹⁶⁸ There, the court similarly held that the Sherman Act prohibited acts having a harmful effect within the United States, even if the parties completed those acts outside the United States.¹⁶⁹ Because the defendant's actions in threatening patent infringement suits in foreign countries restrained trade in the United States, the court ruled that the United States had subject matter jurisdiction per the effects test.¹⁷⁰

Similarly, the court in *Ivanov* properly determined that the effect of Ivanov's conduct in the United States gave U.S. courts jurisdiction, even though Ivanov was physically in Russia.¹⁷¹ Although Ivanov used a complex computer process that he controlled from Russia, Ivanov purposefully accessed the OIB company's computer without authorization and obtained the valuable data in the United States, which the CFAA prohibits.¹⁷² Moreover, similar to *Mannington*, Ivanov

164. *Id.* at 422.

165. 15 U.S.C. § 1 (2000).

166. *Alcoa*, 148 F.2d at 444-45; see *United States v. Nippon Paper Indus.*, 109 F.3d 1, 1-2, 9 (1st Cir. 1997) (finding jurisdiction over a group of Japanese fax paper suppliers who held meetings solely in Japan to fix prices of paper in North America).

167. *E.g.*, *Cont'l Ore Co. v. Union Carbide & Carbon Corp.*, 370 U.S. 690, 704 (1962) (holding that the Canadian respondent was not outside the reach of the Sherman Act just because part of the activity took place outside the United States, so long as the activity's effects are felt within the United States); *Steele v. Bulova Watch Co.*, 344 U.S. 280, 288 (1952) (holding that *Am. Banana Co. v. United Fruit Co.*, 213 U.S. 347 (1909), did not confer a blanket immunity on activities which "radiate unlawful consequences" in the United States even if those activities were initiated outside the country); *Timberlane Lumber Co. v. Bank of Am., N.T. & S.A.*, 549 F.2d 597, 610-12 (9th Cir. 1976).

168. 595 F.2d 1287 (3d Cir. 1979).

169. *Id.* at 1291-92.

170. *Id.* at 1290.

171. 175 F. Supp. 2d 367, 370-71 (D. Conn. 2001).

172. *Id.* at 371-72. More, specifically, an individual violates the CFAA if he or she knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4) (2000). OIB's computers were "protected" under the CFAA definition because OIB used them in interstate commerce. 18 U.S.C. § 1030(e) (defining protected computers).

threatened to damage OIB's computers, which the CFAA also prohibits.¹⁷³ OIB received this threat in Connecticut about their computers located in Connecticut.¹⁷⁴ Just as in *Mannington* where the defendant made threats in a foreign country but the threats had their effect in the United States,¹⁷⁵ Ivanov made the threat from a computer in Russia, but the actual effect manifested itself in the United States. Because Ivanov accessed a specific computer in the United States and threatened a particular company's computer system, the effects were sufficiently particularized and foreseeable to give the United States jurisdiction under the effects test.¹⁷⁶

In addition, Ivanov intended such effects. Ivanov intended to obtain the data and move it to his computer in Russia.¹⁷⁷ He could not do this without affecting OIB's computers in the United States. As a result, the *Ivanov* court properly applied the CFAA extraterritorially, not only because of the language and history of the statute, but also because Ivanov's actions had their intended and actual effect in the United States.

In the embedded software scenario, a court can similarly find that it has subject matter jurisdiction over a charge brought against the Chinese programmer under the CFAA.¹⁷⁸ In this scenario, a programmer in China introduces malicious code into embedded software that the U.S. company exports back to the United States. Similar to *Ivanov*, even though the programmer inserts the malicious code into the embedded software product in China, if the product is physically in the United States when the malicious code executes, it renders its damaging effects in the United States.¹⁷⁹ Although the Chinese programmer may only generally know that the embedded software would be exported to the United States, but not exactly where in the United States, this does not defeat subject matter jurisdiction.¹⁸⁰

173. 18 U.S.C. § 1030(a)(7) ("Whoever . . . with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer . . . shall be punished as provided in subsection (c) of this section."); *Ivanov*, 175 F. Supp. 2d at 372.

174. *Ivanov*, 175 F. Supp. 2d at 372.

175. 595 F.2d 1287, 1290 (3d Cir. 1979).

176. *Ivanov*, 175 F. Supp. 2d at 372.

177. *Id.* at 370-72.

178. *See id.* at 370-71.

179. So long as the product containing the embedded software is considered a protected computer, the U.S. company or U.S. government can bring a claim under the CFAA against the programmer. *See* 18 U.S.C. § 1030(e) (defining a protected computer).

180. *Id.*

The specificity required from the antitrust jurisprudence is specificity of harm, not of location.¹⁸¹ For example, the court in *Alcoa* discussed the restriction on imports as restrictions on imports into the United States generally that affected the prices in the United States as a whole.¹⁸² Similarly, the court in *Timberlane Lumber Co. v. Bank of America N.T. & S.A.*¹⁸³ addressed the effect on “external trade and commerce of the United States” in discussing the attempt to prevent the export of lumber into the United States.¹⁸⁴ Neither case discussed an effect on a particular U.S. location but, rather, looked to the specific harm on the U.S. market overall.¹⁸⁵ Likewise, by introducing malicious code into embedded software exported to the United States, the Chinese programmer affects specifically the party in the United States who uses that embedded software, even though the location in the United States is not specifically known to the programmer.

Furthermore, embedded software is usually tailored to a specific product.¹⁸⁶ Thus, the programmer must understand the particular product to know how to introduce the malicious code.¹⁸⁷ If the programmer does not know specifically how to make the malicious code work in relation to the embedded software product, the malicious code may not execute. As such, in the embedded software scenario there is a greater specificity of harm than in the antitrust cases.¹⁸⁸ The agreements in the antitrust cases discussed target prices or higher market power but not necessarily a particular price or percentage of market power.¹⁸⁹ In contrast, a particular piece of

181. *Accord* *Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1291-92 (3d Cir. 1979) (holding that threatening to bring patent infringement suits in foreign countries restricted trade in the United States); *see* *United States v. Aluminum Co. of Am. (Alcoa)*, 148 F.2d 416, 444 (2d Cir. 1945) (finding that the cartel’s general agreement to restrict production had the specific effect of limiting imports into the United States);

182. *Alcoa*, 148 F.2d at 443-44.

183. 549 F.2d 597 (9th Cir. 1976).

184. *Id.* at 611.

185. *Timberlane Lumber Co. v. Bank of Am., N.T. & S.A.*, 549 F.2d 597, 609-11 (9th Cir. 1976); *Alcoa*, 148 F.2d at 443-44.

186. *See, e.g., Lee, Embedded Software, supra* note 1, at 2 (asserting that embedded software is closely related to and is constrained by the device into which the software is programmed).

187. *See Lee, What’s Ahead, supra* note 1, at 19 (explaining that the embedded software developer is also an expert in the particular device for which he or she is programming).

188. *E.g., Timberlane Lumber*, 549 F.2d at 609-11 (finding harm to the lumber market generally); *Alcoa*, 148 F.2d at 422 (describing a general harm to aluminum competition in the United States).

189. *E.g., Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1290, 1292 (3d Cir. 1979) (holding that the U.S. courts had jurisdiction because the threats to bring patent infringement suits could be seen as an attempt to monopolize the

malicious code, which the programmer inserts into the product, causes the specific harm in the embedded software scenario.

However, for the effects test to apply, the plaintiff must prove that the Chinese programmer intended to cause harm in the United States.¹⁹⁰ The plaintiff could prove this intention by showing that the programmer likely knew that the product would be exported back to the United States due to the company structure and business model, including the influence of U.S. culture and language in daily activities.¹⁹¹ Although a joint venture or WFOE could possibly sell embedded software products in China, in the embedded software scenario, the company employs programmers in China but exports the products back to the United States as part of the business model.

market); *Alcoa*, 148 F.2d at 422, 443-44 (ruling that the agreement to restrict imports was equivalent to price fixing, which is prohibited by the Sherman Act).

190. *Bersch v. Drexel Firestone, Inc.*, 519 F.2d 974, 989 (2d Cir. 1975); *Alcoa*, 148 F.2d at 444 (holding that the cartel intended to restrict aluminum imports and exports through its agreement).

191. *See* Chen, *supra* note 27, at 10 (explaining that foreign invested enterprises such as WFOEs and joint ventures are required to be set up for a specific purpose); Daniel C.K. Chow, *The Limited Partnership Joint Venture Model in the People's Republic of China*, 30 LAW & POL'Y INT'L BUS. 1, 10-12 (1998) (arguing that joint ventures between U.S. and Chinese partners often encounter management-style or decision conflicts and suggesting that, at the outset of establishing the joint venture, the U.S. company make clear through specific agreements and governance structure that it will have the main role in the management and operational decision-making for the enterprise). *But cf.* Rules for Implementation of WFOEs P.R.C., *supra* note 33, at art. 15 (requiring the name of the business for the application but not specifying what the name must include). Additionally, assuming that the U.S. company that is offshore sourcing to China has already established operations in the United States, some knowledge transfer will need to take place between the U.S. company and the Chinese counterpart. CARMEL & TJIA, *supra* note 8, at 130-31. This knowledge transfer forces explicit interaction between the U.S. employees and Chinese employees to transfer knowledge areas such as skills, processes, and work norms. *Id.* at 131. Furthermore, the U.S. company will set up a governance structure between its Chinese counterpart and itself. This includes detailing the hierarchy, setting goals, and developing a relationship. *Id.* at 141. Knowledge transfer activities, setting up the governance structure, and implementing the governance structure heavily involve the participation of the U.S. company and employees with the Chinese employees. Thus, the Chinese employees are likely to know they are working for a U.S.-based company. In addition, offshore sourcing often encounters cross-cultural issues. *See* S. Krishna et al., *Managing Cross-Cultural Issues in Global Software Outsourcing*, COMM'NS OF THE ACM, Apr. 2004, at 62, 64 (providing examples of cross-cultural differences that are evident in outsourcing relationships such as preferring written agreements over verbal, social behavior, attitude toward authority, and language); Mendel, *supra* note 8, at 259 (acknowledging the presence of language and cultural differences even when the U.S. company sets up a subsidiary in China); *see also* CARMEL & TJIA, *supra* note 8, at 176-80 (showing that in the power orientation index by Geert Hofstede and Edward Hall, U.S. employees are forty points lower than Chinese, meaning that hierarchy is very important to the Chinese and they are less likely to question managers; in addition, in the relationship orientation index, there is a seventy-one point difference, U.S. employees view themselves as highly individualistic, Chinese employees view themselves as highly collectivistic).

If the U.S. company makes clear its scope of business and takes an active role in daily operations, it is likely that the Chinese programmer would be aware that some of the products will be exported back to the United States.¹⁹² By programming malicious code into an embedded software product the programmer knew was likely destined for the United States, the Chinese programmer intended for the malicious code to affect the United States. Therefore, a court can use the effects test to exercise subject matter jurisdiction over the CFAA claim against the Chinese programmer.¹⁹³

3. *The conduct test may also be used to find subject matter jurisdiction*

A person may, in some instances, commit acts within the United States that a U.S. law may prohibit, but the consummation and effects of those acts are outside of the United States.¹⁹⁴ Particularly in some securities fraud cases, a court cannot find jurisdiction using the effects test because the harm is to non-U.S. citizens, even though the actions furthering the securities fraud occurred in the United States.¹⁹⁵ The conduct test, also called the subjective territorial principle, allows a court to find jurisdiction when significant conduct occurs in the United States that furthers a fraud or crime that Congress intended to prohibit, while taking into account the sovereignty of foreign nations.¹⁹⁶

192. Cf. Chow, *supra* note 191, at 10-12 (suggesting that the U.S. company take an active role in the joint venture to avoid conflicts in any decision making).

193. See *supra* notes 190-193 and accompanying text (showing how a plaintiff could show harm necessary to meet the effects test standard).

194. See *Leasco Data Processing Equip. Corp. v. Maxwell*, 468 F.2d 1326, 1334 (1972) (stating that while a court has jurisdiction over conduct occurring in another country but has effects within the United States, it also has jurisdiction over significant conduct within the United States that relates to the harm, even if the harm is in another country).

195. See *Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 667 (7th Cir. 1998) (finding jurisdiction over a Caribbean corporation for fraudulently inducing a Malaysian corporation to invest in satellite technology because the Caribbean corporation used the United States as a base of operations to further the fraud); *Timberlane Lumber Co. v. Bank of Am., N.T. & S.A.*, 549 F.2d 597, 611-12 (9th Cir. 1976) (“The effects test by itself is incomplete because it fails to consider other nations’ interests.”); *Leasco*, 468 F.2d at 1334 (acknowledging that the harmful effects in the case did not manifest within the United States); *supra* Part III.C.2 (discussing the effects test).

196. See, e.g., *Cont’l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 421-22 (8th Cir. 1979) (“[W]e decline to immunize, for strictly jurisdictional reasons, defendants who unleash from this country a pervasive scheme to defraud a foreign corporation.” (citation omitted)); *Hamlin*, *supra* note 132, at 378-79 (describing the conduct test as the subjective territorial principle). See generally RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 416 (1987) (summarizing that, as it has developed in the United States with respect to the regulation of securities, the conduct test permits the United States to prescribe conduct related to any transaction in securities carried out in the United States,

The conduct within the United States must be significant and it must be an essential or material link to the completion of the fraud or crime to find jurisdiction.¹⁹⁷ While the conduct within the United States cannot be “merely preparatory” or simply a “failure to prevent fraudulent acts where the bulk of the activity was performed in foreign countries,”¹⁹⁸ the conduct does not necessarily have to satisfy the elements of the final fraud or crime for a court to find jurisdiction.¹⁹⁹

Courts will find extraterritorial jurisdiction when the defendant uses the United States as a base of operations.²⁰⁰ For example, Section 10(b) prohibits the use of the U.S. mail system to perpetrate fraud on investors.²⁰¹ In *IIT v. Vencap, Ltd.*,²⁰² the court ruled that the defendants, a company incorporated in the Bahamas, could be charged with violating section 10(b) even though the majority of the investors were not U.S. citizens because they used the U.S. mail system to perpetrate a fraud on investors.²⁰³ The court stated that it did not believe that Congress intended the United States to be a “base for manufacturing fraudulent security devices for export, even when these are peddled only to foreigners.”²⁰⁴

More recently, the court in *Kauther* used almost identical reasoning of the conduct test to find subject matter jurisdiction over section 10(b) claims against the defendants.²⁰⁵ The court stated that it had jurisdiction if the conduct in the United States is substantial and has a direct link to the loss. As a result, the court held that the plaintiffs sufficiently alleged that the defendants used the United States as a

whether or not the security is traded on an organized securities market). A court can also use this test in conjunction with the language and history of the statute, with the effects test, or as an individual test. *See Cont'l Grain*, 592 F.2d at 416-17 (agreeing that jurisdiction may be established by meeting the requirements of either the subjective or objective territorial principles, or both).

197. *Leasco*, 468 F.2d at 1334.

198. *Cont'l Grain*, 592 F.2d at 418, 420.

199. *Kauther*, 149 F.3d at 667.

200. *See, e.g., IIT v. Vencap, Ltd.*, 519 F.2d 1001, 1017-18 (2d Cir. 1975). *See generally* Barbara S. Thomas, *Extraterritoriality in an Era of Internationalization of the Securities Markets: The Need to Revisit Domestic Policies*, 35 RUTGERS L. REV. 453, 455 (1983) (summarizing how most U.S. courts have determined that Congress did not intend for the United States to be used as a base of operations for fraudulent activity even if the effect of the activity is felt outside the United States).

201. 15 U.S.C. § 78j(b) (2000); 17 C.F.R. § 240.10b-5 (2007).

202. 519 F.2d at 1001.

203. *Id.* at 1018 (“[L]iterally hundreds of transactions and pieces of mail for Vencap and to a lesser extent for Intervent and Intercapital were initiated, directed and consummated from and received at 99 Park Avenue.”).

204. *Id.* at 1017.

205. *Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 665, 667 (7th Cir. 1998).

base of operations to defraud Kauther and sent the fraudulent material through the U.S. mail.²⁰⁶

Even if the United States is not a base of operations, frequent use of the U.S. mail system can be enough for the United States to have jurisdiction.²⁰⁷

In *Continental Grain (Australia) Pty. Ltd. v. Pacific Oilseeds, Inc.*,²⁰⁸ the court found subject matter jurisdiction over a 1934 Securities Act claim because the defendant's conduct in the United States furthered its fraudulent scheme.²⁰⁹ The court found that conduct in the United States, which consisted of letters and telephone calls necessary to organize and complete the fraud,²¹⁰ were not "merely preparatory."²¹¹

Although the court in *United States v. Ivanov*²¹² did not find jurisdiction based on the conduct test, such a finding was possible.²¹³ First, the court could consider that the United States was a base of operations for Ivanov. Once Ivanov was in the United States, by accessing OIB's computers, he transferred data from the OIB computers to his computer in Russia.²¹⁴ This conduct was similar to the defendants in *Vencap* and *Kauther* who used offices in the United States to prepare and mail fraudulent material to investors.²¹⁵ Because Ivanov used the OIB computers located in the United States as the base to prepare the data and transmit it to Russia,²¹⁶ his actions satisfy the conduct test.

In addition, Ivanov used the U.S. infrastructure as a means to complete his crime. The *Ivanov* court found that when Ivanov accessed OIB's computers, the access occurred at OIB's location in Connecticut.²¹⁷ This effectively places Ivanov in the United States. Just as the defendants needed to use the U.S. mail system in *Continental Grain* to complete their fraud,²¹⁸ Ivanov needed to access the OIB computers to transfer the data and transmit the threat to

206. *Id.*

207. *Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 420-21 (8th Cir. 1979).

208. 592 F.2d 409 (8th Cir. 1979).

209. *Id.* at 420.

210. *Id.*

211. *Id.*

212. 175 F. Supp. 2d 367, 373 (D. Conn. 2001).

213. *See id.* (finding jurisdiction based on statutory interpretation and the effects test).

214. *Id.* at 371-72.

215. *See Kauther SDN BHD v. Sternberg*, 149 F.3d 659, 665 (7th Cir. 1998); *IIT v. Vencap, Ltd.*, 519 F.2d 1001, 1017-18 (2d Cir. 1975).

216. *Ivanov*, 175 F. Supp. 2d at 371-72.

217. *Id.* at 371.

218. *Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 420 (8th Cir. 1979).

OIB.²¹⁹ Without the U.S. infrastructure in *Continental Grain* or the OIB computers in *Ivanov*, neither defendant could complete his crime.²²⁰

Finding subject matter jurisdiction using the conduct test for the embedded software scenario is admittedly more difficult than finding jurisdiction using the effects test. The embedded software scenario assumes that the programmer is located in China and programs the malicious code in China.²²¹ Therefore, unlike the defendants in *Kauther* or *Vencap*, the United States is not a base of operations for the Chinese programmer.²²²

A court could apply the conduct test to the embedded software scenario if it takes a broad view of “access” under the CFAA. A court has the freedom to find that the programmer in China “accesses” a computer in the United States through the malicious code because “access” is not statutorily defined and courts differ in their interpretations of the term.²²³ The significant and essential conduct in the United States that furthers the programmer’s goals is the “access” via the malicious code in the embedded software that has been exported from China to the United States.

Although in the embedded software scenario the access does not occur in real time,²²⁴ the Chinese programmer uses the U.S. infrastructure to introduce the malicious code into the country. This is similar to the defendants in *Continental Grain* who had to use the U.S. infrastructure to send the fraudulent investment material.²²⁵

219. *Ivanov*, 175 F. Supp. 2d at 371.

220. *See id.*; *Cont'l Grain*, 592 F.2d at 420.

221. *See supra* Introduction (setting up the embedded software scenario).

222. In addition, it is unlikely the court would hold the U.S. parent company responsible for the acts of the employee in China. A court can normally hold a corporation responsible for criminal acts of its employees if the employee acts under the actual or apparent authority of the corporation and for the corporation’s benefit. *United States v. Automated Med. Labs. Inc.*, 770 F.2d 399, 406-07 (4th Cir. 1985). This is true even if the corporation explicitly prohibits the act. *E.g.*, *United States v. Hilton Hotels Corp.*, 467 F.2d 1000, 1004-05, 1007 (9th Cir. 1972) (demonstrating that compliance efforts alone do not immunize the corporation from liability). In contrast, the court in *Butera v. IBM* held specifically that it could not apply the CFAA to the corporation if the corporation did not explicitly authorize the employee’s action. 456 F. Supp. 2d 104, 110 (D.D.C. 2006). Therefore, a court could not find subject matter jurisdiction based solely on the conduct of the U.S. company in the United States, unless the U.S. company actively participated in programming the malicious code.

223. *See* 18 U.S.C. § 1030(e) (2000) (defining several other terms in the statute, but not defining “access”); *see also* Kerr, *supra* note 87, at 1617-21 (criticizing the lack of definition); *supra* Part III.A (discussing definition of “access”).

224. *Contra Ivanov*, 175 F. Supp. 2d at 369, 371-72 (describing the real time hacking by Ivanov).

225. *Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 419 (8th Cir. 1979).

Without the U.S. infrastructure, the Chinese programmer could not introduce the malicious code into the United States. Just as the court in *Continental Grain* found subject matter jurisdiction because the defendant used the U.S. infrastructure in furtherance of a fraudulent scheme,²²⁶ a court in the embedded software scenario could find jurisdiction with similar reasoning.

Even though a court could find jurisdiction by using the conduct test, statutory interpretation and the effects test are the strongest bases for extending the CFAA extraterritorially and finding subject matter jurisdiction in the embedded software scenario.²²⁷ However, by its nature, extraterritorial application of a U.S. law infringes on the sovereignty of foreign nations to police and judge their own citizens.²²⁸ As the jurisprudence of antitrust and securities law demonstrates, courts attempt to balance the interest of the United States with that of the foreign nation when deciding whether to exercise jurisdiction.²²⁹

D. International Comity Considerations Support Subject Matter Jurisdiction

While a court can find subject matter jurisdiction over a CFAA claim against a Chinese programmer from the language and history of the statute, the effects test, the conduct test, or a combination of the three approaches, there may be policy reasons why it should not do so in a particular case. In some situations, the interest to preserve harmony with the foreign country can outweigh the interest of the United States in pursuing jurisdiction.²³⁰ In the embedded software scenario, however, the balance of international comity weighs in favor

226. *Id.* at 420.

227. *See supra* Part III.C (analyzing statutory interpretation, effects test, and conduct test).

228. *Accord* *Timberlane Lumber Co. v. Bank of Am., N.T. & S.A.*, 549 F.2d 597, 613 (9th Cir. 1976) (stating that in addition to analyzing whether there was a sufficiently large effect on American foreign commerce, the court must also address whether the “magnitude of the effect on American foreign commerce are (sic) sufficiently strong, vis-a-vis those of other nations”). *Timberlane’s* analysis for when anticompetitive conduct in foreign nations can provide subject matter jurisdiction for an antitrust suit in U.S. courts has been superseded by statute. *See* 15 U.S.C. § 6a (1982) (providing a subject matter jurisdiction test for conduct involving trade with foreign nations). The principles of international comity that the court discusses, however, are still relevant. *See Timberlane*, 549 F.2d at 613-14 (balancing many factors in deciding jurisdiction).

229. *See Timberlane*, 549 F.2d at 613-14 (listing the elements that should be taken into account when balancing the interests of the foreign nation); *see also* *SEC v. Kasser*, 548 F.2d 109, 116 (3d Cir. 1977) (analyzing policy considerations for exercising jurisdiction after holding that the defendant’s conduct allowed the court to find jurisdiction).

230. *Timberlane*, 549 F.2d at 609.

of finding subject matter jurisdiction over a CFAA claim against a Chinese programmer.²³¹

1. *The jurisdictional rule of reason approach leads to exercising subject matter jurisdiction*

One primary approach to balancing a foreign country's sovereignty with U.S. jurisdiction is the jurisdictional rule of reason test.²³² The court in *Timberlane* explained the factors a court should weigh to balance the other country's interest; these include: (1) "the degree of conflict with foreign law or policy," (2) the nationality of the parties and the locations of the businesses, (3) the ability of either state to enforce compliance, (4) "the relative significance of effects on the United States as compared with those elsewhere," (5) the extent of the explicit purpose to harm U.S. commerce, (6) the foreseeability of the harmful effect or conduct, and (7) "the relative

231. See Alford, *Extraterritorial Antitrust Laws*, *supra* note 132, at 37 ("[T]he U.S. approach essentially grants courts the *right* to assert jurisdiction as broadly as international law permits, but then gives them the *discretion* to refuse to exercise this right in the interest of international comity."); see also Douglas E. Rosenthal, *Relationship of U.S. Antitrust Laws to Formulation of Foreign Economic Policy, Particularly Export and Overseas Investment Policy*, 49 ANTITRUST L.J. 1189, 1193-94 (1980) (suggesting that the Department of Justice took a case-by-case approach to asserting extraterritorial jurisdiction, particularly for antitrust cases, in the 1970s). See generally RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 (1987) (limiting the jurisdiction to prescribe if it would be "unreasonable"). The Restatement lists the following eight factors to consider in determining reasonableness:

- (a) the link of the activity to the territory of the regulating state, *i.e.*, the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;
- (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;
- (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;
- (d) the existence of justified expectations that might be protected or hurt by the regulation;
- (e) the importance of the regulation to the international political, legal, or economic system;
- (f) the extent to which the regulation is consistent with the traditions of the international system;
- (g) the extent to which another state may have an interest in regulating the activity; and
- (h) the likelihood of conflict with regulation by another state.

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2). It then cautions that the list is not exhaustive and that no priority should be given to any one factor. *Id.* § 403 cmt. b.

232. *Timberlane*, 549 F.2d at 614.

importance to the violations charged of conduct within the United States as compared with conduct abroad.”²³³ After assessing these factors and the potential conflict between the United States and the foreign country, if the United States asserts jurisdiction, the court should then determine whether the interests of the United States are sufficient to support the exercise of extraterritorial jurisdiction.²³⁴

Using the jurisdictional rule of reason test, the court in *Timberlane* found subject matter jurisdiction appropriate.²³⁵ Even though most of the antitrust activity took place in Honduras, the defendants likely organized the conspiracy from San Francisco, which affected competition and commerce in the United States.²³⁶ In addition, U.S. antitrust law did not conflict with the law or policy of Honduras.²³⁷ The court was also not concerned about the harmony of relations between the United States and Honduras if a U.S. court exercised jurisdiction in the matter.²³⁸

Whether a court should exercise subject matter jurisdiction in a particular embedded software scenario will vary depending on the exact nature of the crime.²³⁹ Certain factors from the jurisdictional rule of reason do weigh in favor of finding jurisdiction in the embedded software scenario.

First, similar to *Timberlane*, there is no conflict with Chinese law.²⁴⁰ Chinese law does not require a programmer to insert malicious code into embedded software. In fact, a court can legitimately read the Chinese Criminal Code to prohibit such conduct, making the U.S. and Chinese criminal laws similar.²⁴¹ Even if a court does not read the

233. *Id.*; see *Mannington Mills, Inc. v. Congoleum Corp.*, 595 F.2d 1287, 1297-98 (3d Cir. 1979) (reiterating and adding to the *Timberlane* factors but holding that the factual record was not sufficient to make a finding about the factors).

234. *Timberlane*, 549 F.2d at 614-15; cf. Harold G. Maier, *Extraterritorial Jurisdiction at a Crossroads: An Intersection Between Public and Private International Law*, 76 AM. J. INT'L L. 280, 317 (1982) (positing that it is difficult for a U.S. court to objectively balance the interest of another country with that of the United States, thus making the jurisdiction rule of reason test unworkable).

235. *Timberlane*, 549 F.2d at 615.

236. *Id.*

237. *Id.*

238. *Id.*

239. See *Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 421-22 (8th Cir. 1979) (holding that the United States had jurisdiction when considering international comity); *Timberlane*, 549 F.2d at 614-15 (finding that the U.S. court had jurisdiction after weighing all the factors to determine whether finding jurisdiction would conflict with foreign law or policy).

240. See *Timberlane*, 549 F.2d at 615 (“[T]here has been no indication of any conflict with the law or policy of the Honduran government.”).

241. Specifically, the Chinese Criminal Code article 286 states in relevant part:

Whoever . . . cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally . . . Whoever intentionally creates or spreads destructive programs

Chinese Criminal Code as such, the Code does not appear to encourage such acts.²⁴² Thus, a court could not find a conflict of law to weigh against jurisdiction.²⁴³

Second, due to the lack of ensured prosecution in China, it is more likely the U.S. judicial system can effectively adjudicate its computer crime law, both civilly and criminally.²⁴⁴ Third, all effects from the

such as the computer viruses, thus affecting the normal operation of the computer system . . . shall be [sentenced to fixed-term imprisonment]. Criminal Law of the People's Republic of China (promulgated by National People's Congress, Mar. 14, 1997, effective Oct. 1, 1997), art. 286, *available at* <http://www.lawinfochina.com/law/dispecontent.asp?db=1&id=354> (P.R.C.) [hereinafter Criminal Code P.R.C.]. *See generally* WEI LUO, 1997 CRIMINAL CODE, *supra* note 117, at 8 (interpreting 1997 Criminal Code, Article 3, to state that only crimes that are defined explicitly in the Code are crimes; a person cannot be found guilty by an analogous law).

242. *See generally* Criminal Code P.R.C., *supra* note 241, at arts. 4, 286 (stating that any offender of an act explicitly defined in the law shall be punished, and prohibiting the spread of computer viruses); WEI LUO, 1997 CRIMINAL CODE, *supra* note 117, at 16 (listing as one of the major new offenses added to the 1997 Criminal Code to be "computer frauds (Article 285-286)").

243. *See Timberlane*, 549 F.2d at 615 (citing a lack of a conflict of law as a factor supporting jurisdiction).

244. *See supra* note 131 (noting that the power to adjudicate and the power to enforce are separate and therefore although a U.S. court could rule against a Chinese national, there may still be an issue of enforcing the judgment). Despite China's recent progress and accession to the World Trade Organization (WTO), litigating in China still concerns U.S. companies. *E.g.*, U.S. TRADE REPRESENTATIVE, 2004 REPORT TO CONGRESS ON CHINA'S WTO COMPLIANCE 3 ("China deserves due recognition for the tremendous efforts made to reform its economy to comply with the requirements of the WTO."); Mei Ying Gechlik, *supra* note 46, at 97-98 (criticizing China's courts for lacking fairness and justice but noting that Beijing has begun to take steps to improve the judicial system); Mo Zhang, *Int'l Civil Litigation in China: A Practical Analysis of the Chinese Judicial System*, 25 B.C. INT'L & COMP. L. REV. 59, 63 (2002). One of the reasons for the concern is that few Chinese laws are published in English, and the Chinese judicial system is complex for someone unfamiliar with it. *See* Sylvia Ostry, *Article X and the Concept of Transparency in the GATT/WTO, in CHINA AND THE LONG MARCH TO GLOBAL TRADE*, *supra* note 46, at 128 (noting the "multilayered complexity" of the Chinese legal system and reviewing the various types of laws, including internal administrative laws and generalized laws issued by the National People's Congress); *see also* WEI LUO, CHINESE LAW AND LEGAL RESEARCH 164-65 (2005) (reviewing the history of the Chinese publishing industry, which was essentially shut down during the Cultural Revolution but between the 1980s and 2000 grew from a little over forty thousand titles to over one hundred and forty three thousand titles). Lawyers and scholars also recognize problems within the Chinese judicial system, which has suffered from interference by the Chinese Communist Party ("CCP") leaders. Mei Ying Gechlik, *supra* note 46, at 100-01 (reporting that, as of 2005, interference into the judiciary from party officials was still a major obstacle in litigation); Yuwen Li, *Court Reform In China: Problems, Progress and Prospects*, in IMPLEMENTATION OF LAW IN THE PEOPLE'S REPUBLIC OF CHINA 58-59 (Jianfu Chen et al. eds., 2002) (listing lack of judicial independence as a major problem of the judicial system and reporting that courts often make decisions on cases according to the "instructions of the leaders of the Communist Party" and the government). The central government and CCP leadership have a large influence on the local courts, which in turn facilitates pushing the judges to conform their judgments to the social and legal ideals of the CCP. *See* Mei Ying Gechlik, *supra* note 46, at 136 (explaining that this influence is a fundamental problem with the court system); *see*

malicious code will be in the United States, none in China. Finally, these effects are explicit and foreseeable in causing harm to the United States. All these factors combine to weigh in favor of exercising subject matter jurisdiction.²⁴⁵

2. *Policy considerations also permit exercising jurisdiction*

A court does not have to rely on the *Timberlane* factors to balance jurisdiction with international comity, but can look to other policy considerations to examine this balance.²⁴⁶ One line of reasoning suggests that if the U.S. exercises jurisdiction for conduct within its borders but with the ultimate effects felt abroad, it encourages other countries to find and exercise jurisdiction when conduct occurs in the foreign country but has its effects in the United States, thus further protecting the United States.²⁴⁷ In addition, if there is no conflict with the other country's laws, then a court can often find jurisdiction without further consideration.²⁴⁸

A second line of reasoning suggests that if a court can discern from the statute or the legislative history an intent on the part of Congress to prohibit a specific action within the United States, then the balance will favor finding jurisdiction.²⁴⁹ If Congress designed a law to protect certain groups in the United States, then a court will tend

also Biddulph, *supra* note 46, at 176 (explaining that courts and judges in China have a lower status and lack financial independence from the local government, which hampers the judges' independence to rule on cases). As such, a U.S. company is not guaranteed fairness and the relative predictability it is accustomed to in the United States if it uses Chinese courts to litigate. *See, e.g.*, Biddulph, *supra* note 46, at 156 (noting that there is still unease about the relationship between law and policy set by the ruling Chinese Communist Party).

245. *See Timberlane*, 549 F.2d at 614 (listing factors for determining when subject matter jurisdiction should be exercised). Factors that weigh in favor of not exercising jurisdiction include the fact that the programmer is a Chinese citizen and that China does have a law apparently prohibiting the spread of computer viruses. In addition, a court should take into account the current political relationship with China at the time the case arises. *See id.*

246. *See, e.g.*, SEC v. Kasser, 548 F.2d 109, 116 (3d Cir. 1977) (articulating three general policy rationales for finding jurisdiction); *see also* Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc., 592 F.2d 409, 421-22 (8th Cir. 1979) (using policy rationales from *Kasser* to support finding jurisdiction).

247. *See Kasser*, 548 F.2d at 116 ("By finding jurisdiction here, we may encourage other nations to take appropriate steps against parties who seek to perpetrate frauds in the United States."); *see also* Cont'l Grain, 592 F.2d at 421 (stating that finding jurisdiction will encourage other nation's courts to find jurisdiction when a fraud takes place in the United States).

248. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 797-99 (1993) (determining that there was no conflict with British law).

249. *See Kasser*, 548 F.2d at 116 (noting that the purpose of the statute was to protect the domestic market from fraud and finding jurisdiction would conform with that purpose); *see also* Cont'l Grain, 592 F.2d at 421 (agreeing with the rationale articulated by the *Kasser* Court).

to find jurisdiction. In *SEC v. Kasser*,²⁵⁰ the court held that Congress designed the antifraud provisions of the securities acts to ensure “high standards of conduct in securities transactions” in the United States and protect “investors from the effects of fraud.”²⁵¹ Moreover, the court found that the legislative intent was to prevent the United States from becoming a “haven” for defrauders and manipulators.²⁵² Similarly, in *Continental Grain*, the court held that finding jurisdiction was consistent with the intent of Congress to encourage high standards of conduct in the investment market and not to use the United States as a base of operations.²⁵³

Furthermore, in both *Kasser* and *Continental Grain* the courts also held that by finding jurisdiction it would encourage other countries “to take appropriate steps against parties who seek to perpetrate frauds in the United States.”²⁵⁴ While both policy reasons need not be present, they offer alternative reasoning to the factor test set out in *Timberlane*.

More recently, in *Hartford Fire Insurance Co. v. California*,²⁵⁵ the Supreme Court found that “international comity would not counsel against exercising jurisdiction” based on a comparison of U.S. and British law.²⁵⁶ The Court focused solely on the fact that British law did not force the London insurance providers to violate U.S. law, even though the providers’ actions would have been legal in London.²⁵⁷ The Court held that simply because conduct is lawful in the country in which it takes place, it does not prevent extraterritorial application of U.S. antitrust laws “even where the foreign state has a strong policy to permit or encourage such conduct.”²⁵⁸ Thus, there was no conflict of U.S. and British laws to weigh against exercising jurisdiction, which was the only conflict the Court felt it needed to consider.²⁵⁹

Applying the non-*Timberlane* international comity approaches to the embedded software scenario, a court can still exercise subject matter jurisdiction. First, Congress designed the CFAA to punish

250. 548 F.2d at 109.

251. *Id.* at 116.

252. *Id.*

253. *Cont'l Grain*, 592 F.2d at 421.

254. *See Kasser*, 548 F.2d at 116; *see also Cont'l Grain*, 592 F.2d at 421 (hoping that finding jurisdiction would lead to reciprocal enforcement abroad).

255. 509 U.S. 764 (1993).

256. *Id.* at 798.

257. *Id.* at 797-99.

258. *Id.* at 799.

259. *Id.*; *cf. Alford, Extraterritorial Antitrust Laws, supra* note 132, at 19 (describing the Hartford ruling and criticizing the Court for its lack of concern for “the legitimate sovereignty interests of another country that may have concurrent jurisdiction”).

those who access a protected computer without authorization.²⁶⁰ While there is still debate on the exact definition of “access” and “authorization,” the 1996 Senate Report noted Congress’s concern for computers used in foreign commerce that were vulnerable to hackers located in foreign countries.²⁶¹ Just as Congress intended the securities acts to protect investors from general fraud and to encourage high standards in the investment market,²⁶² the CFAA protects computer users from unwanted access and encourages those with knowledge about computer systems to use their knowledge to improve technology, not to harm others.²⁶³

Second, finding jurisdiction over a Chinese citizen for violating the CFAA may encourage China to find jurisdiction over its own citizens who attempt to cause harmful effects in the United States. Additionally, if exercising jurisdiction in the securities cases can encourage a higher standard for investment markets internationally,²⁶⁴ then finding jurisdiction in the embedded software scenario can encourage a higher standard for ensuring software security. Third, and more directly, using the *Hartford Fire* analysis, so long as there is no conflict between U.S. law and Chinese law, there is no need to further examine international comity principles.²⁶⁵ Because a Chinese programmer could comply with both Chinese law and U.S. law by not programming malicious code into the embedded software, international comity would not preclude jurisdiction over a CFAA claim.²⁶⁶

In sum, a court can use the jurisdictional rule of reason factor analysis to determine whether it should exercise subject matter jurisdiction in the embedded software scenario or a more generalized

260. See S. REP. NO. 104-357, at 3-5 (1996) (stating that the goal was to have a single statute to address all computer crimes).

261. See *id.* at 4-5; see also *United States v. Ivanov*, 175 F. Supp. 2d 367, 374 (D. Conn. 2001) (using the 1996 Senate Report to support its finding of extraterritorial jurisdiction).

262. See, e.g., *Cont'l Grain (Austl.) Pty. Ltd. v. Pac. Oilseeds, Inc.*, 592 F.2d 409, 421 (8th Cir. 1979); *SEC v. Kasser*, 548 F.2d 109, 116 (3d Cir. 1977).

263. See 18 U.S.C. § 1030 (2000) (prohibiting computer fraud and abuse).

264. *Accord Cont'l Grain*, 592 F.2d at 421 (agreeing with the *Kasser* analysis); see *Kasser*, 548 F.2d at 116 (reasoning that finding jurisdiction would make it more likely that foreign courts would also find jurisdiction, creating a more effective securities regulation regime).

265. See *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 798-99 (1993) (holding that there was no conflict between British and American Law because the party could abide by both laws simultaneously).

266. See *id.* at 798-99 (reasoning that there is only a conflict if a party cannot abide by both laws simultaneously). See generally RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE U.S. § 403(2)(h) (1987) (listing the likelihood of conflict with regulations of another state as a factor in analyzing whether a U.S. court should exercise jurisdiction).

policy consideration approach. Either method will take into account the United States' relationship with China and its own interests in protecting American citizens and businesses yet still result in finding subject matter jurisdiction.²⁶⁷

CONCLUSION

U.S. businesses looking to source work in China and the U.S. government have an interest in ensuring the security of embedded software designed and built in China. In addition to incorporating protective language into private contracts and choosing U.S. law in foreign related contracts, extending the Computer Fraud and Abuse Act extraterritorially allows the United States to prosecute or sue a Chinese citizen who chooses to program malicious code into embedded software, even though that person is physically located in China. Following the reasoning of antitrust and securities fraud cases, the CFAA can be applied extraterritorially because of its statutory language and history; because the effects of the malicious code in the United States is substantial; and because conduct furthering the violation of the CFAA occurred in the United States. The extraterritorial application of the CFAA also acts as a deterrent to any programmer who would program malicious code into embedded software developed in China, and it serves as a remedial tool for any malicious code that has already made its way to the United States. Therefore, even acknowledging that there may be some security risk to developing embedded software overseas, there is no need to restrict offshore sourcing to China.

267. *Supra* notes 232-34, 247-59 and accompanying text.