THE ECONOMIC ESPIONAGE ACT—REVERSE ENGINEERING AND THE INTELLECTUAL PROPERTY PUBLIC POLICY†

*Craig L. Uhrich**

Cite as: Craig L. Uhrich, *The Economic Espionage Act—Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. TECH. L. REV. 147 (2001), *available at* http://www.mttlr.org/volseven/uhrich.html.

† An earlier draft of this Article received the 2000 Mark Vela Award for the best paper in criminal law at the University of Houston.

* B.S., Kansas State University, 1992; M.B.A., University of Houston—Victoria, 1999; J.D. magna cum laude, University of Houston Law Center, 2000; LL.M. International Legal Studies, N.Y.U. School of Law, 2001. I would like to thank Professor Geraldine Szott Moohr, from whom I learned criminal law, for her continuing guidance throughout the development of this Article. I also would like to thank Professors Paul M. Janicke and Rochelle Cooper Dreyfuss and Ms. Heidi K. Wambach and Mr. Kevin M. Ashby for their assistance in reviewing and commenting on drafts of this Article. All errors are mine. In addition, I would like to thank Scott Cook for preparing and distributing this Article. Finally, I would like to thank my family and friends, especially Donna Coleman, Jason and Aimée Hinshaw, Neal Pellis, Randy Pryor, Brian White, and Robert Wichmann, for their continued support of me in my professional endeavors.

INTRODUCTION

In 1992, Ronald Hoffman was caught selling software to Japanese industrial firms.[1] He had obtained the software through his position as a project manager for Science Applications, Inc., which had developed the programs under a secret contract with the Strategic Defense Initiative.[2] Hoffman had been selling confidential information to Japanese companies since 1985.[3]

In 1995, Pierre Marion, the former head of French intelligence, admitted that hotel rooms of businessmen staying in Paris routinely were broken into.[4] The purpose of these break-ins was to copy proprietary business papers.[5] This information then was provided to French companies to give them a competitive advantage.[6]

In the early part of the decade, Marc Goldberg and Jean Safar, both French nationals, were arrested for trying to sell proprietary computer source codes of their employer, Renaissance Software.[7] Both men were working with the company under an official French government program that allowed citizens to opt out of required military service if they agreed to work at American high-tech companies.[8]

The publicity surrounding these and other incidents of industrial espionage resulted in a push for federal protections.[9] In response to this pressure from U.S. industries, Congress passed the Economic Espionage Act of 1996 ("EEA").[10] The EEA protects trade secrets through the use

1. *See* 142 CONG. REC. S12,201, S12,210 (1996) (statement of Sen. Specter) [hereinafter *Specter-1*] (incorporating Peter Schweizer, *The Growth of Economic Espionage: America is Target Number One*, FOREIGN AFF., Jan./Feb. 1996).

2. *See id.* (recalling Hoffman's activities and noting their chronological proximity to the highly publicized activities of a KGB mole within the CIA).

3. *See id.*

4. *See* 142 CONG. REC. S377 (1996) (statement of Sen. Cohen) [hereinafter *Cohen*] (recalling Marion's statement that as many as fifteen rooms were broken into every day).

5. *See id.*

6. *See id.*

7. *See Specter-1*, *supra* note 1, at S12,209 (recounting the arrests).

8. *See id.*

9. *See* Gerald J. Mossinghoff et al., *The Economic Espionage Act: A Prosecution Update*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 360, 360 (1998) (noting the concerns over industrial espionage).

10. 18 U.S.C. §§ 1831–39 (1999).

of federal criminal sanctions.[11] The EEA's provisions are introduced in Part I.[12]

Trade secrets are a form of intellectual property.[13] Therefore, a basic understanding of intellectual property law is important to an analysis of the EEA. Part II of this Article provides an overview of the various forms of intellectual property.[14]

To be effective, the EEA must complement existing intellectual property jurisprudence. Yet, on its face the EEA prohibits practices that are otherwise lawful as part of a reverse engineering program. Part II of this Article also describes reverse engineering and examines its acceptance in each area of intellectual property law.[15]

Understanding the EEA in terms of the other forms of intellectual property protection and the practice of reverse engineering raises some concerns over the prudence of vigorous EEA enforcement. A strict reading of the EEA may prohibit reverse engineering. Since reverse engineering plays a significant role in the exploitation of knowledge committed to the public domain through the grant of patents and copyrights, prohibiting reverse engineering may stifle the drive to study and improve upon the existing knowledge base. Part III of this Article examines these concerns.[16]

The increasing importance of intellectual property in the world economy has created a trend toward criminalization of infringement. In addition to the acts covered by the EEA, some international agreements require criminal sanctions for infringement of various rights,[17] certain acts of copyright infringement carry criminal penalties,[18] and Congress is currently considering the Collections of Information Antipiracy Act.[19]

---

11. *See* 18 U.S.C. § 1831(a)(5) (1999) (providing for a term of imprisonment of fifteen years where the espionage is to benefit a foreign entity). If the espionage is for the benefit of an American company, the sentence is ten years. *See* 18 U.S.C. § 1832(a)(5) (1999).

12. *See infra* notes 22–43 and accompanying text.

13. *See* Rockwell Graphics Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) ("trade secret protection is an important part of intellectual property").

14. *See infra* notes 44–177 and accompanying text.

15. *See infra* notes 66–78 and accompanying text.

16. *See infra* notes 178–304 and accompanying text.

17. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Annex 1, art. 61, 108 Stat. 4809, 4833, 33 I.L.M. 81, 105 (requiring member states to provide criminal penalties for "wilful [sic] trademark counterfeiting or copyright piracy").

18. *See infra* notes 90–91 and accompanying text (discussing criminal copyright provisions).

19. Collections of Information Antipiracy Act, H.R. 354, 106th Cong. §§ 1402(a), 1407 (1999) (providing for prison terms up to ten years for persons extracting or making available "all or a substantial part of" a collection of information that is created or maintained "through the investment of substantial . . . resources"). It has been argued that, to the extent it will protect unoriginal information, Congress lacks the Constitutional power to enact this bill [formerly H.R. 2652]. *See* William Patry, *The Enumerated Powers Doctrine and*

While these laws are designed to protect intellectual property, the inclusion of criminal sanctions means that they must be analyzed in light of criminal law theories such as notice, vagueness, and leniency. As this trend continues, and prosecutions under these new laws become more frequent, it will be important for criminal practitioners to have a firm grasp of intellectual property concepts and for intellectual property attorneys to understand the importance of criminal law. Finally, it is important for Congress to consider such criminal law issues when enacting new intellectual property legislation. A discussion of these issues with respect to the EEA provides a framework for developing this discussion with respect to other intellectual property laws.

To assist in determining the legitimacy of these concerns, Part III also examines the legislative history of the EEA to ascertain congressional intent with respect to the identified problems.[20] Based upon the issues raised in Part III, Part IV proposes a solution to address these concerns while maintaining the effectiveness of the EEA in fulfilling its intended purpose.[21] Specifically, the Article proposes amending the EEA to explicitly allow reverse engineering and to limit its application to espionage activities similar to those Congress had in mind when drafting the Act.

I. THE ECONOMIC ESPIONAGE ACT

As the value of information continues to increase,[22] American businesses are becoming more concerned about industrial espionage conducted by foreign entities.[23] Following the end of the Cold War, foreign governments increasingly employed the resources of their military intelligence agencies to obtain confidential business information.[24] These agencies are engaged in activities such as bugging the airline seats of business passengers and burglarizing their hotel

Intellectual Property: An Imminent Constitutional Collision, 67 GEO. WASH. L. REV. 359, 394–98 (1999).

20. *See infra* notes 189–216 and accompanying text.

21. *See infra* notes 288–304 and accompanying text.

22. *See* Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921, 922 (1989) (noting the significant growth in the political, social, and economic power of information).

23. *See* DAVID R. SIMON & FRANK E. HAGAN, WHITE-COLLAR DEVIANCE 83–85 (1999) (reporting that the government-operated Japan External Trade Organization is considered to be among "the most sophisticated commercial-intelligence gathering" organizations in the United States).

24. *See* 142 CONG. REC. S12,201, S12,211 (1996) (statement of Sen. Kohl) [hereinafter *Kohl-1*] (noting that the several high technology industries are "aggressively targeted" for espionage activities); Lederman, *supra* note 22, at 928.

rooms.[25] A survey conducted among security directors of businesses that were members of the American Society of Industrial Security (ASIS) suggested that forty-eight percent of their companies had experienced trade secret theft in 1987.[26] ASIS data revealed that trade secret theft cost American businesses $25 billion between 1992 and 1995.[27] The number of cases of economic espionage being investigated by the FBI in 1996 showed a 200% increase over those being investigated two years earlier.[28]

Though the theft of trade secrets is prohibited by state law, there is considerable disparity among the trade secret laws of the various states.[29] This disparity laid the foundation for industry demands for a uniform, national regime of trade secret protection.[30] Finally, in response to several documented cases of foreign espionage and an alarming increase in reports of corporate trade secret theft, Congress enacted the EEA.[31] The EEA provides criminal penalties for the misappropriation of trade secrets.[32] These penalties may be broad enough to require the forfeiture of computers used to transmit trade secrets via email.[33]

The EEA establishes a broad list of intangible properties that can form the basis of a trade secret.[34] The EEA's definition of a trade secret

25. *See* SIMON & HAGAN, *supra* note 23, at 84 (reporting that the French *Direction Generale de la Securite Exterieure*—previously used to spy on other nations—is the most active military intelligence agency currently gathering confidential business information).

26. *See id.* at 85 (reporting further that 90% of the survey participants had experienced such theft during the previous ten years).

27. *See id.* at 83; *Specter-1*, *supra* note 1, at S12,211 (stating estimates of losses to American businesses resulting from intellectual property theft exceed $100 billion).

28. *See* SIMON & HAGAN, *supra* note 23, at 83 (noting 800 pending investigations in 1996). The data, however, does not reveal how much of this increase is the result of heightened awareness, rather than increased spying.

29. *See infra* notes 145–59 and accompanying text.

30. *See* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 179–187 (1997) (noting the concerns the EEA was drafted to address); *see also* S. REP. NO. 104-359, at 10–11 (1996) (citing shortcomings of federal and state protections).

31. *See* Mossinghoff et al., *supra* note 9, at 360 (reviewing the Congressional atmosphere under which the EEA was passed).

32. *See* 18 U.S.C. § 1831 (1996) (establishing a 15-year prison term for espionage benefiting a foreign party); 18 U.S.C. § 1832 (1996) (establishing a ten year prison term for theft of trade secrets); 18 U.S.C. § 1834 (1996) (requiring forfeiture of property used in the crime).

33. *See* 18 U.S.C. § 1834 (1996); *see also* 1 MELVIN F. JAGER, TRADE SECRETS LAW § 4.01[4][b] (1999) (outlining the possibility for seizure of computers used for Internet transmission).

34. *See* 18 U.S.C. § 1839(3) (1996) (defining trade secrets to include "all forms and types of financial, business, scientific, technical, economic, or engineering information").

is very similar to that of the Uniform Trade Secrets Act (UTSA).[35] In keeping with state trade secret law, the EEA also requires that the owner of the property takes affirmative steps to protect its secrecy.[36] Once the vague conditions for the existence of a trade secret are met, the EEA criminalizes three broad categories of activities, as well as conspiracy to commit an offense within the categories.[37] The actions outlawed include (i) theft, concealment, or destruction; (ii) sketching, copying, or transmittal; and (iii) receipt of misappropriated trade secrets.[38] It is worth noting that the misappropriation prohibited by the EEA is broader than that prohibited by the UTSA.[39] Though the EEA allows the Attorney General to bring a civil action for an injunction,[40] it does not provide for private, civil causes of action for federal trade secret misappropriation.[41]

Several criticisms have been raised against the EEA.[42] The most interesting with respect to traditional intellectual property law is the possible prohibition of reverse engineering, which is typically allowed in other arenas of intellectual property law.[43] As will be discussed below, the degree to which reverse engineering is prohibited is not entirely clear. Even the lack of clarity surrounding the legality of

35. *See* United States v. Hsu, 40 F. Supp. 2d 623, 628 (E.D. Pa. 1999) (noting only "minor modifications" to the definition contained in the UTSA). *Compare* 18 U.S.C. § 1839(3) *with* UNIF. TRADE SECRETS ACT § 1(1), 14 U.L.A. 437 (1990) (defining trade secrets to include only "information, including a formula, pattern, compilation, program, device, method, technique, or process"). Since trade secret law varies amongst the states, the trade secret law used throughout this Article is generally based on the UTSA.

36. *See* 18 U.S.C. § 1839(3)(a) (1996).

37. *See* 18 U.S.C. § 1832 (1996); 1 JAGER, *supra* note 33, § 4.01[4][b] (examining the EEA's scope).

38. *See* 18 U.S.C. § 1832 (1996). The EEA seems to adopt the property theory of trade secrets. *See* Pooley et al., *supra* note 30, at 193 (noting that the EEA does not require the existence of a confidential relationship).

39. *See* United States v. Martin, 228 F.3d 1, 19 (1st Cir. 2000) ("This definition of trade secret 'protects a wider variety' of information than most civil laws") (quoting United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998)). *Compare* UNIF. TRADE SECRET ACT § 1, 14 U.L.A. 437 (1990) (defining misappropriation as acquisition or disclosure of a trade secret by "improper means," through a breach of duty to maintain secrecy, or with knowledge that it is a trade secret that was released by mistake) *with supra* text accompanying note 38. *See also* Pooley et al., *supra* note 30, at 187–88 (describing the misappropriation provisions as "entirely new and [with] no parallels in existing trade secrets law").

40. *See* Brown v. Citicorp, No. 97 CV 6337, 1998 WL 341610, at *3 n.3 (N.D. Ill. 1998) (mem.) (citing 18 U.S.C. 1836 (1994 & Supp. 1998)).

41. *See* 18 U.S.C. §§ 1831–39 (1996).

42. *See generally* Pooley et al., *supra* note 30 (criticizing the EEA for potentially allowing licensee actions to forfeit trade secret status, arguably being of little use against computer hackers because it incorporates traditional criminal law "conversion" language that may preclude prosecution of those acting with non-economic motives, and failing to allow for reverse engineering).

43. *See id.* at 195 (noting the absence of a reverse engineering defense).

reverse engineering, however, can be expected to lead to a chilling of these creative efforts.

II. INTELLECTUAL PROPERTY AND REVERSE ENGINEERING

Intellectual property can be defined simply as proprietary information and other kinds of assets that give business enterprises a competitive advantage.[44] Chemical formulas, customer lists, design tolerances, and production processes are typical examples of intellectual property.[45] Depending on its type, intellectual property derives its value from a bundle of nearly exclusive rights defined by statute,[46] common law,[47] or contract.[48]

Intangible property historically has been an anomaly in the criminal law.[49] Since it is not a physical asset, intellectual property has been difficult to protect under the traditional theories of prosecution.[50] Traditional property crimes generally require a taking or a carrying away of the property in question.[51] Intellectual property, however, is

---

44. *See* WILLIAM C. HOLMES, INTELLECTUAL PROPERTY & ANTITRUST LAW § 2.01 (2000) (describing trade secrets).

45. *See id.*; 1 DONALD S. CHISUM, CHISUM ON PATENTS § OV[1] (2000).

46. *See, e.g.*, 35 U.S.C. §§ 1–376 (2000) (patent law); KAN. STAT. ANN. § 60-3320 (1999) (Kansas trade secret law).

47. *See, e.g.*, Hickory Specialties, Inc. v. B&L Labs., Inc., 592 S.W.2d 583, 586–87 (Tenn. App. 1979) (citing Allis-Chalmers Mfg. Co. v. Continental Aviation & Eng. Corp., 255 F. Supp. 645 (E.D. Mich. 1966) and Smith v. Dravo Corp., 203 F.2d 369 (7th Cir. 1953)); Softel, Inc. v. Dragon Med. & Scientific Communications, Inc., 118 F.3d 955, 968 (2d Cir. 1997) ("New York generally looks to Section 757 of the First Restatement of Torts for its definition of a trade secret.").

48. *See, e.g.*, K&G Oil Tool & Serv. Co. v. G&G Fishing Tool Serv., 314 S.W.2d 782 (Tex. 1958) (upholding trade secret protection based on equipment lease provisions). *See also* 1 JAY DRATLER, JR., LICENSING OF INTELLECTUAL PROPERTY § 1.05[1] (1999) (describing rights provided by various forms of intellectual property).

49. *See infra* notes 50–57 and accompanying text (discussing these difficulties).

50. *See* Christopher A. Ruhl, Note, *Corporate & Economic Espionage: A Model Penal Code Approach for Legal Deterrence to Theft of Corporate Trade Secrets & Proprietary Business Information*, 33 VAL. U. L. REV. 763, 780 (1999) (noting the limited usefulness of mail and wire fraud statutes to protect trade secrets); *see also* Peter J. Toren, *Internet: A Safe Haven for Anonymous Information Thieves?*, 11 ST. JOHN'S J. LEGAL COMMENT. 647, 649–50 (1996) (discussing the difficulty of prosecuting the transmission of stolen computer information across state lines because, as intangible property, it does not meet the "goods, wares, or merchandise" requirement). *See generally* Randy Gidseg et al., *Intellectual Property Crimes*, 36 AM. CRIM. L. REV. 835 (1999) (studying the application of a range of crimes to various forms of intellectual property).

51. *See* Gidseg et al., *supra* note 50, at 843 (noting the traditional view that the National Stolen Property Act (NSPA) will apply to trade secrets only when they are stolen in tangible form); Toren, *supra* note 50, at 651 (recalling that thieves no longer need to physically copy protected information because they can access it remotely and transmit copies over large distances).

intangible,[52] and, as such, not limited to a single physical manifestation. For example, the owner can reproduce an unlimited number of products containing his intangible property without giving up the original.[53] As a result, when an infringer makes a copy of a protected work the owner still has use of the item.[54] Because the owner retains his copy, it is difficult to characterize the infringer's act as a carrying away.[55] The only deprivation suffered by the owner is exclusivity of use;[56] the property was not carried away.[57]

The civil law provides relief for unauthorized uses of intellectual property.[58] These protections trace their history back to the Middle Ages, when monarchs granted monopolies to cities and merchant guilds allowing them to practice and regulate commerce in their product.[59] These monopolies also were granted to individuals who introduced a product to the kingdom's economy through invention or foreign discovery.[60] Because of abuses experienced during Queen Elizabeth's reign,[61] the English parliament passed the "Statute against Monopolies" that abolished monopolies not granted because of invention or foreign discovery.[62]

---

52. *See* BLACK'S LAW DICTIONARY 831 (deluxe ed. 1999).

53. *See, e.g.*, Geraldine Szott Moohr, *Federal Criminal Fraud & the Development of Intangible Property Rights in Information*, 2000 U. ILL. L. REV. 683, 692–93 [hereinafter *Federal Criminal Fraud*] (contrasting the example of a cake recipe, from which an unlimited number of cakes (and copies of the recipe) can be made without taking the original recipe away from the owner, with the cake itself, which only can be eaten by a limited number of people).

54. *See* Gidseg et al., *supra* note 50, at 857 (noting that prosecutions of copyright infringement under the NSPA fail because there is no physical removal).

55. *See id.*; Lederman, *supra* note 22, at 933 (reporting that information was traditionally only protected when "embodied in some concrete, tangible entity . . . which [was] carried away.").

56. *See Federal Criminal Fraud*, *supra* note 53, at 693 (explaining that loss of exclusive use may, among other consequences, decrease the owner's ability to sell the information).

57. *See* Ruhl, *supra* note 50, at 774–75 (reporting the difficulty in sustaining a NSPA prosecution relating to intangible property).

58. *See infra* notes 136–59 and accompanying text (describing these protections).

59. *See* 1 ANTHONY WILLIAM DELLER, WALKER ON PATENTS 2–6 (1937) (recalling history of European monopolies); 1 WILLIAM C. ROBINSON, THE LAW OF PATENTS FOR USEFUL INVENTIONS § 2, at 4 (Boston, Little, Brown, & Co. 1890) [hereinafter *Patents*] (noting resources amassed by the Hanseatic League through monopolies granted its members).

60. *See* 1 *Patents*, *supra* note 59, § 9 (discussing two classes of English monopolies).

61. *See id.* §§ 5–6 (recalling the Crown's tendency to grant monopolies to favored subjects who would sell them to merchants and then to grant to monopoly owners the power to search and collect penalties). During Elizabeth's reign, salt prices increased from 16 pence to 15 shillings a bushel. *See id.* § 6.

62. *See id.* § 7.

The United States Constitution grants the federal government the authority to protect intellectual property.[63] Congress has used this power to confer intellectual property rights through patents and copyrights.[64] Since it does not fit within the traditional federal scheme of granting protection in exchange for adding information to the public domain, trade secret protection has been left to the states to regulate.[65]

A. *Reverse Engineering*

The purpose of intellectual property protection is to provide incentives to invest and to advance the collective knowledge. Therefore, the law recognizes exceptions that allow for the study of, and improvement upon, discoveries that have been committed to the public domain, in all realms of intellectual property protection.[66] Reverse engineering is one of these exceptions.[67] Reverse engineering is the process of studying an item in hopes of obtaining a detailed understanding of the way in which it works.[68] Reverse engineering is used to create duplicate or superior products without the benefit of

63. *See* U.S. CONST. art. I, § 8, cl. 8 (granting Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries").

64. *See generally* 17 U.S.C. §§ 101–121 (1994) (copyrights); 35 U.S.C. §§ 100–105, 271–296 (1994) (patents); 17 U.S.C. §§ 901–912 (1998) (maskworks). The federal government also provides protections to registered trademarks. *See* 15 U.S.C. §§ 1111–1128 (1994). Trademarks, however, do not possess the properties of most of the intellectual properties discussed in this paper. *See* 1 JEROME GILSON, TRADEMARK PROTECTION & PRACTICE §§ 1.03[1]&[2] (1992) (noting the functions of, and policies behind, trademark protection are based on the consumers' need to distinguish goods of different manufacturers). The first trademark statute, which was partially based on the Constitution's patent clause, was found to be unconstitutional. *See* United States v. Steffens, 100 U.S. 82, 94 (1879) (holding the law to be unconstitutional because trademarks had "no necessary relation to invention or discovery"). Therefore, federal protection of trademarks is now based on the commerce clause. *See* 15 U.S.C. § 1051(a) (1994) (requiring an application for trademark registration to disclose the date the mark was first used in commerce); 1 GILSON, *supra*, § 1.04[3][b] (noting the requirement that the trademark to be registered must "contact with interstate commerce").

65. *See* 1 JAGER, *supra* note 33, § 2.03 (noting the scarcity of United States Supreme Court trade secret cases because trade secrets are the product of state law). It is worth noting that the EEA also protects financial and economic data that do not fall under the Constitutional grant of promoting the useful arts. Therefore, the protection of this type of data must be based on the interstate commerce power.

66. *See* 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.05[5] (1999) (summarizing the legality of such study with respect to patents, copyrights, and trade secrets).

67. *See id.*

68. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (defining reverse engineering as "starting with the known product and working backward to divine the process which aided in its development or manufacture").

having the plans for the original item.[69] While reverse engineering can occur in a variety of situations, it is not an excuse for illegal activities. For example, one could dissect and study a secret prototype that had been obtained through burglary or armed robbery. Such an activity, however, would not be legal simply because it was part of a reverse engineering scheme. For the purposes of this Article, the discussion of the legality of reverse engineering will always assume the item being reverse engineered was legally obtained.

It is important, however, to understand that reverse engineering is not just a scheme to allow copying under the guise of research.[70] Reverse engineering, while it may involve copying, entails a detailed study of the item in question.[71] Even in cases where the end product is a near duplicate of the original item, the purpose of the reverse engineering activities must have been to understand the item sufficiently to allow the accused party to redesign the product without resort to step-by-step replication.[72] Since, as in the case of computer chips, any differences between the original and the new product may be infinitesimal, courts typically rely on the existence of a "paper trail" to prove that the product was reverse engineered, rather than simply copied.[73]

Depending on the nature of the item under study, reverse engineering may take many forms. For mechanical devices such as turbines or cargo containers, reverse engineering may consist of taking measurements, making detailed sketches, or disassembling the device.[74] In the case of computer chips, the process involves stripping away each layer of the chip to study the structure of the layer.[75] To ensure that the reverse engineering process is accurate, a duplicate is often made.

---

69. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989) ("Reverse engineering . . . often leads to significant advances in technology.").

70. *See* Brooktree Corp. v. Advanced Micro Devices, Inc., 977 F.2d 1555, 1570 (Fed. Cir. 1992) (finding the accused infringer to have copied, rather than reverse engineered, the maskwork).

71. *See id.* at 1567.

72. *See, e.g.*, 17 U.S.C. § 906(a) (Supp. 1998) (providing a defense to infringement of a protected maskwork where the reproduction was "solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied"); *see also* Atari Games Corp. v. Nintendo of America Inc., 975 F.2d 832, 845 Fed. Cir. 1992 (finding that the replication of unnecessary instructions in the resulting computer code was evidence of copying, not independent creation resulting from reverse engineering).

73. *See Brooktree*, 977 F.2d at 1567 (reviewing the requirements for a reverse engineering defense).

74. *See* Pooley et al., *supra* note 30, at 195 (asserting that reverse engineering may involve activities prohibited under the EEA).

75. *See Brooktree*, 977 F.2d at 1565.

Though vendors may take steps to make reverse engineering more difficult, the process is commonly accepted within the scientific community.[76] Reverse engineering is also implicitly accepted in patent, copyright, and state trade secret laws.[77] Federal maskwork protection laws explicitly allow for the reverse engineering of computer chips.[78]

B. *Copyrights*

Copyrights protect the expressions of ideas in various forms.[79] The ideas themselves, however, are not protected.[80] For example, an artist may set an easel in front of a work of art and paint a work inspired by the first without violating copyright law.[81] A copyright grants the owner the exclusive right to copy or import the protected material and the right of first publication.[82] This right of first publication grants the author the right to determine "when, where, and in what form" the work is first published.[83] Copyright protection applies to ideas memorialized in a tangible medium—written publications, works of art, certain recordings, and performances.[84] Copyright protection also has been partially extended to computer programs.[85]

Infringement of a copyright will be found where the accused work was copied from and is *substantially similar* to the copyrighted work.[86] The test for substantial similarity is whether an ordinary person would recognize the accused item as having been copied from the protected

---

76. *See supra* notes 66–67 and accompanying text. The reverse engineering provision in the Semiconductor Chip Protection Act was lobbied for by the chip industry because they felt that reverse engineering, as a step toward new chip designs, was more efficient. *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 291 n.219 (1998).

77. *See infra* notes 103, 123–24, & 160 and accompanying text.

78. *See* 17 U.S.C. § 906(b) (1994).

79. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 350 (1991) (stating that a factual compilation is copyrightable only if it "features an original selection or arrangement").

80. *See* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 547 (1985) ("no author may copyright facts or ideas").

81. *See* Alfred Bell & Co. v. Catalda Fine Arts, Inc., 191 F.2d 99, 103 (2d Cir. 1951) (holding that independent reproductions of a copyrighted work was not infringement and could itself be granted a copyright); *see also* 17 U.S.C. § 103 (1994) (allowing for the copyright protection of derivative works).

82. *See* 17 U.S.C. § 106 (1998) (setting forth the rights of a copyright owner).

83. *See Harper & Row*, 471 U.S. at 564.

84. *See* 17 U.S.C. § 102 (1994) (requiring that the work of authorship be fixed in a tangible medium in order to be afforded copyright protection).

85. *See* 17 U.S.C. § 117 (1994).

86. See Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586–91 (1994) (finding that a rap music parody of a copyrighted work did not infringe the copyright because, among other things, of a lack of substantial similarity).

work.[87] Furthermore, exceptions to copyright protection are made for copying which falls within the fair use doctrine.[88] Infringement of a copyright imposes civil remedies including destruction of the infringing items, damages, recovery of lost profits, and assessment of attorneys' fees.[89] Copyright law also provides criminal sanctions for certain types of infringement.[90] Unlike the EEA, however, the maximum term of imprisonment for a first offense is limited to five years.[91]

Since a copyright does not protect the underlying idea, issues of reverse engineering rarely arise in the context of artistic creations. The important issues of copyright protection and reverse engineering arise in the case of copyrighted computer programs.[92] In this area, the Digital Millennium Copyright Act explicitly provides a reverse engineering defense to allow competitors to develop compatible programs.[93] For acts falling outside of this provision, decompiling is often accepted under copyright law as a form of fair use.[94]

Generally speaking, computer programs are sets of mathematical algorithms used to instruct the computer in its functions.[95] Mathematical

87. *See* Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1166–67 (1977) (finding that the McDonald Land characters were "substantially similar" to the characters of the popular children's television show H.R. Pufnstuf). In applying this test, the court determined that the nature of the target audience—children, in this case—must be taken into account. *See id*.

88. *See generally Acuff-Rose Music*, 510 U.S. 569 (analyzing the accused infringer's fair use defense); *see also* 17 U.S.C. § 107 (1994) (providing the considerations to be analyzed for a fair use defense).

89. *See* 17 U.S.C. §§ 502–505 (1994) (providing remedies for infringement).

90. *See* 17 U.S.C. § 506 (1994) (providing penalties for criminal infringers).

91. *See* 18 U.S.C. § 2319(b)(1) (2000).

92. Some discussion of reverse engineering with respect to copyrights occurs in cases involving computer technology. *See, e.g.*, DSC Communications Corp. v. DGI Techs., Inc., 81 F.3d 597, 600–02 (5th Cir. 1996) (discussing the concept of copyright misuse as it applies to copyrighted circuit boards).

93. *See* Digital Millennium Copyright Act of 1998, 17 U.S.C. § 1201(f) ("Reverse engineering . . . a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure . . . for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability. . . .").

94. *See, e.g.*, Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 609 (9th Cir. 2000) (allowing reverse engineering of a game console operating system in an effort to create compatible game cartridges); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514 (9th Cir. 1993) (holding that disassembly of a copyrighted computer code was, as a matter of law, fair use where the person had a legitimate reason to disassemble the code and where no other means of access existed); Atari Games Corp. v. Nintendo of America Inc., 975 F.2d 832, 843 (Fed. Cir. 1992) ("Thus, reverse engineering object code to discern the unprotectable ideas in a computer program is a fair use.").

95. *See* Gottschalk v. Benson, 409 U.S. 63, 67 (1972) (discussing a patent application for a program to convert binary numbers).

algorithms are difficult to protect as intellectual property.[96] As a result, the source code of a computer program, which consists of the base algorithms in readable form, is not protectable by patent law, but may be protectable by copyright law.[97] Though the object code—the machine-readable version of the program that is distributed to customers—is not directly readable, development of the copyright law has made programs, as distributed in object code form, subject to copyright.[98]

As the source code is protected, simply copying the program would be an act of infringement.[99] To be able to read and understand the program's logic, a programmer must decompile the object code to reveal an undocumented source code.[100] This process involves making intermediate copies of the program.[101] Though these intermediate copies fall within the purview of copyright protection,[102] decompiling a program so that the source code can be studied and a competing program can be written is a form of reverse engineering that enjoys wide acceptance because it is required to open the program to investigation.[103]

---

96. *See id.* (recalling that "abstract intellectual concepts" are not patentable because they are the basic tools of scientific work).

97. *See id.* at 71–73 (rejecting patent claims covering "the programmed conversion of numerical information" from one encoding format to another as a practical patent on the base algorithm). *Cf.* Diamond v. Diehr, 450 U.S. 175, 191–93 (1981) (ruling that a patent could be granted for an industrial process incorporating computer program control based upon a well-known mathematical formula). *See also* Stern Elecs., Inc. v. Kaufman, 669 F.2d 852, 855–57 (Fed. Cir. 1982) (discussing the copyright protection of computer programs as literary or audiovisual works); Robert H. Lande & Sturgis M. Sobin, *Reverse Engineering of Computer Software and U.S. Antitrust Law*, 9 HARV. J.L. & TECH. 237, 242 (1996) (discussing issues in the copyright protection of computer programs).

98. Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1248–49 (3d Cir. 1983) (protecting computer program source code and object code as literary work). *See generally* Anthony J. Mahajan, *Intellectual Property, Contracts, and Reverse Engineering After* ProCD*: A Proposed Compromise for Computer Software*, 67 FORDHAM L. REV. 3297, 3299–303 (1999) (describing the concerns relating to and the emergence of computer program copyright protection).

99. *See* 17 U.S.C. § 106(1) (1998) (granting the copyright owner the exclusive right to copy or authorize the work).

100. Lande & Sobin, *supra* note 97, at 240–42 (describing the reverse engineering of computer programs and object code).

101. *Id.* at 241 ("[I]t is impossible to undertake the process of decompilation without at some point making a copy of either some or all of the program.").

102. *See* Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 602–03(9th Cir. 1993) (recalling that intermediate copying could constitute copyright infringement even when the end product does not contain protected material (citing Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1518–19 (9th Cir. 1992))).

103. Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832, 842–44 (Fed. Cir. 1992) (noting the constitutional objective of promoting "the Progress of Science" and concluding that necessary intermediate copies for object code reverse engineering are

C. *Patents*

Patents protect inventions.[104] To qualify for a patent, the device must meet the statutory requirements of novelty[105] and non-obviousness.[106] Under the novelty requirement, the patent applicant must show that he or she was the first in a WTO country to invent the claimed subject matter of the application without subsequently abandoning, suppressing, or concealing it.[107] The patent law also requires that the inventor act diligently in applying for patent protection. For example, if the device is publicly used in this country more than one year prior to the filing of the patent application, the invention will be considered to be part of the public domain and the patent will be denied.[108]

If a patent is granted, the owner possesses a monopoly over the product extending from the issue date to twenty years after the date of the initial application a twenty-year monopoly over the product.[109] This monopoly gives the patent holder the right to exclude others from making, using, selling, or importing any product covered by a claim of the patent.[110] Infringers are subject to civil damages that may cover the patentee's lost profits or reasonable royalties for the product.[111] Willful infringement can result in treble damages.[112] In determining infringement, the patent owner is held to the definitions of the property that were given in the "claims" portion of the approved patent

---

exempted from protection by fair use). *See* Lande & Sobin, *supra* note 97, at 243–47 (examining the intellectual property concerns that favor reverse engineering); Mahajan, *supra* note 98, at 3315–19 (noting that patent, copyright, and trade secret laws allow reverse engineering absent contract provisions to the contrary).

104. *See* 35 U.S.C. §§ 100–105 (Supp. 1998) (outlining the requirements for patenting an "invention").

105. 35 U.S.C. § 102 (1994) (detailing the "novelty" requirement for patentability).

106. *See* 35 U.S.C. § 103 (Supp. 1998) (detailing the "non-obvious subject matter" requirement for patentability).

107. *See* 35 U.S.C. § 115 (Supp. 1998) (requiring the inventor to submit an oath stating that he believes himself to be the first inventor).

108. 35 U.S.C. § 102(b) (Supp. 1998) (denying patentability if an invention is patented, described in a printed publication, publicly used, or placed on sale more than one year prior to the date of the application).

109. 35 U.S.C. § 154(a)(2) (Supp. 1998) (granting a monopoly extending from the date of issue to twenty years after the earliest application filing date). The WTO Uruguay Round Agreements resulted in legislation altering the length and manner of calculating the term of a patent monopoly. *See* 5 CHISUM, *supra* note 45, § 16.01.

110. 35 U.S.C. § 154(a)(1) (1998). *But see generally* 5 CHISUM, *supra* note 45, § 16.02[1] (cautioning that the right to exclude others does not imply the affirmative right to make, use, or sell oneself because "blocking patents," or federal or state laws, may restrict those activities).

111. 35 U.S.C. § 284 (1998) (providing for damages not less than a reasonable royalty, including interest and costs).

112. *Id.* Attorney fees may be awarded in exceptional cases. 35 U.S.C. § 285 (1998).

application.[113] Items that are not within the patent claims will not be found to literally infringe the patent.[114] Furthermore, the patent law does not provide criminal sanctions for infringing a patent.[115]

The patent law addresses reverse engineering processes as an ancillary issue. A patent gives its owner a monopoly to exclude others from making, using, selling, or importing the patented item.[116] Since the patent law requires an applicant to disclose at least one embodiment of the invention to the public with sufficient detail to allow "one skilled in the art" to make it, reverse engineering is not necessary.[117] With respect to commercial embodiments of patented technology, however, reverse engineering processes may be a consideration in a variety of circumstances.

First, a competitor may wish to design a product to compete with the commercial embodiment.[118] To do this, the competitor will need to design a product that is similar to the product but distinct enough to fall outside the patent claims.[119] In the process of designing around the patent, a competitor may purchase several of the commercially available products and reverse engineer them to get a better understanding of the way they work.[120] Since the competitor is not performing the prohibited acts of making, using, or selling the patented technology, this will not

113. Amstar Corp. v. Envirotech Corp., 730 F.2d 1476, 1481–82 (Fed. Cir. 1984) (explaining that patent infringement is determined by comparing the accused product and the patent claims, not by comparing the accused and patented products).

114. *See id.* Substantially similar items that do not literally infringe the patent claims may be found to infringe under the doctrine of equivalents, which analyzes the role played by each element of the patent claim to determine "whether a substitute element matches the function, way, and result of the claimed element." Warner-Jenkinson Co. v. Hilton Davis Chem. Co., 520 U.S. 17, 40 (1997). The Doctrine of Equivalents can be traced back nearly 150 years. *See id.* at 26 n.3 (discussing the evolution of the doctrine and opposition to it in both Graver Tank & Mfg. Co. v. Linde Air Prods. Co., 339 U.S. 60 (1950) and Winans v. Denmead, 15 How. 330 (1854)).

115. 7 CHISUM, *supra* note 45, § 20.01.

116. *See supra* note 109 and accompanying text.

117. 35 U.S.C. §§ 112–113 (1998) (requiring the inventor to submit a specification containing a written description of the invention and the manner of making and using it, and one or more drawings illustrating the claimed subject matter in most instances); Mahajan, *supra* note 98, at 3317 (prohibiting sale of reverse engineered ideas from patented technology is mitigated by mandatory public disclosure of protected inventions).

118. *See* Mahajan, *supra* note 98, at 3317–18 (undertaking reverse engineering for the purpose of competition, compatibility, or study was unlikely to constitute patent infringement absent other infringing activities).

119. This is referred to as "designing around" the patent. 5A CHISUM, *supra* note 45, § 18.04[1][a][iii] (describing the ability to design around a patent as one of the public benefits that justifies the award of a patent monopoly).

120. *See, e.g.*, Paper Converting Mach. Co. v. Magna-Graphics Corp., 745 F.2d 11, 19–20 (Fed. Cir. 1984) (determining whether competitors may make a patented product, for testing purposes, during the life of a patent). Similarly, reverse engineering may be needed to allow for repair of the patented item.

be a violation. A second situation arises where someone other than the patent-holder wishes to market repair services for the patented product.[121] The competitor may have to dissect the product to understand some of the construction details that are necessary for repairing the item. Finally, the situation may arise where a product is covered by a patent claim, but some features of the commercial embodiment were not included in the patent specifications or drawings.[122] In this case, a competitor may wish to incorporate the non-patented features directly from the commercial embodiment into an item that does not fall within any of the patent's claims.

All of these situations are accepted under current patent law.[123] In fact, a finding that the infringer was engaged in reverse engineering processes in an unsuccessful attempt to design around the claim often will support a finding that the infringement was not willful.[124] This finding will avoid an award of increased damages even though the defendant was infringing.[125]

D. *Maskworks*

Semiconductor maskworks[126] are now protected under the Semiconductor Chip Protection Act.[127] These protections were created in

121. *See, e.g.*, ARO Mfg. Co. v. Convertible Top Replacement Co., 365 U.S. 336, 346 (1961) (allowing repair and reconstruction of patented items after they are sold).

122. *See infra* note 150 and accompanying text (discussing the possibility of trade secret protection complementing patent protection for details outside the specification and drawing requirements of 35 U.S.C. §§ 112–113); Mahajan, *supra* note 98, at 3317 (noting that inventors are not per se required to disclose the source code of a patented computer program).

123. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 146, 156–57 (1989) (noting the careful balance between promoting invention and preserving competition through imitation and refinement established by patentability criteria). State attempts to prohibit the copying of unpatented boat hulls by a direct molding technique through the grant of patent-like protections rejected as a substantial threat to the goals of the patent system). *Id.* at 160–61.

124. *See, e.g.*, Read Corp. v. Portec, Inc., 970 F.2d 816, 828–30 (Fed. Cir. 1992) (overturning jury's finding of willful infringement by a party that attempted to design around competitor's patents and secured an opinion of counsel on non-infringement); Rolls-Royce Ltd. v. GTE Valeron Corp., 800 F.2d 1101, 1108 (Fed. Cir. 1986) (upholding the district court's finding of no willful infringement by a party that attempted to design around competitor's patents, but failed to seek an opinion of counsel on non-infringement).

125. *See supra* note 112 and accompanying text (noting that willful infringement can result in treble damages). There is a tension between the discouragement of willful infringement through copying and the encouragement of competition through "designing around" patents. *See* 7 CHISUM, *supra* note 45, § 20.03[4][v][G]. This tension is magnified in cases involving reverse engineering, since direct copying is a strong element of a case for willful infringement. *See* Kaufman Co. v. Lantech, Inc., 807 F.2d 970, 978–79 (Fed. Cir. 1986) (citing the defendant's statements that he would copy any machine, regardless of patent protection, and defendant's use of admitted equivalents in his machine as facts supporting a finding of willful infringement).

126. A maskwork is a series of stencils used to etch circuits onto the layers of semiconductor material that comprise a chip. *See* 17 U.S.C. § 901(a)(2) (1998).

127. Semiconductor Chip Protection Act of 1984, 17 U.S.C. §§ 901–912 (1998).

response to the difficulties of protecting computer chips under the then-existing protections granted by patents and copyrights.[128] While the chip itself is not protected, the maskwork used to produce the chip is protected.[129] The analysis of infringement under this scheme is very similar to infringement analysis under the copyright laws—including the substantial similarity test.[130]

Computer chips are especially likely candidates for reverse engineering.[131] In the case of chip circuits, competing products often bear a strong resemblance to the original.[132] When the only intellectual property rights in the chip are its maskworks, the owner has little recourse.[133] The Semiconductor Chip Protection Act specifically allows for reverse engineering.[134] To receive the benefit of this allowance, however, the accused infringer must show that the duplicate chip is the product of reverse engineering, rather than blatant, uninformed copying.[135]

E. *Trade Secrets*

Protection of trade secrets traditionally has been a state function.[136] Trade secrets present a problem in the scheme of intellectual property protections. Federal intellectual property protections arise from an agreement between the creator of the property and the government.[137] In this agreement, the creator discloses the property to the public and, in return, the government grants a limited monopoly to exclude others from use of the property.[138]

---

128. H. R. REP. NO. 98-781, at 3–4 (1984), *reprinted in* 1984 U.S.C.C.A.N. 5750, 5752–53.

129. *See* 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8A.02 (1999) (describing maskwork protections under the Act).

130. *See* Brooktree Corp. v. Advanced Micro Devices, Inc., 977 F.2d 1555, 1563–65 (Fed. Cir. 1992) (finding infringement of a protected maskwork).

131. In fact, the reverse engineering provision of the Semiconductor Chip Protection Act was included at the request of the industry. *See supra* note 76.

132. *See, e.g.*, *Brooktree*, 977 F.2d at 1567 (applying the "substantially similar" test from copyright law to determine if the accused product was "original" or represented plagiarism).

133. *See* 2 NIMMER & NIMMER, *supra* note 129, § 8A.06[A] (noting that the exclusive right of reproduction does not attach until the circuit is fixed on a chip).

134. *See* 17 U.S.C. § 906(a) (1998) (creating a defense of reverse engineering for infringement of semiconductor maskworks).

135. *See Brooktree*, 977 F.2d at 1570 (finding infringement despite the defendant's assertion of reverse engineering).

136. *See supra* note 65 and accompanying text.

137. *See* 1 NIMMER & NIMMER, *supra* note 129, § OV (contrasting copyright privileges with their exemptions and compulsory licenses); HOLMES, *supra* note 44, § 1.02 (describing the patent scheme as one to "induce public disclosure" of the invention).

138. *See* HOLMES, *supra* note 44, § 1.02 (discussing the trade-off of patent protection).

On the other hand, trade secret protection stems from the creator's ability to keep the property secret.[139] Revealing the property to the public negates its value as a trade secret.[140] Since the holder of the trade secret does not have to disclose the secret to the public to obtain trade secret protection, it is not generally seen as fitting within the constitutional language of "advancing the useful arts."[141] Indeed, some of the information protected by the EEA clearly falls outside the Constitutional grant of power to promote the useful arts.[142] Instead, trade secret protection is seen as maintaining commercial morality and protecting the owner's "fundamental human right, that of privacy."[143] As a result, trade secret protection is traditionally left to state law.[144] The majority of states and the District of Columbia have adopted some version of the UTSA.[145] States that have not adopted the UTSA follow a protection scheme—whether of statutory or judicial origin—based on the Restatement[146] approach.[147]

---

139. *See* 1 JAGER, *supra* note 33, § 4.01[4][a], at 29 (requiring the owner to "exercise eternal vigilance").

140. *See* Smith v. Dravo Corp., 203 F.2d 369, 376 (7th Cir. 1953).

141. *See* 1 MILGRIM, *supra* note 66, § 1.01[1] (asserting that the purpose of trade secret protection is not to encourage invention, but is "merely [to discourage] breach of faith and reprehensible means of learning another's secrets"); *but see* 1 JAGER, *supra* note 33, § 1.05 (including "the encouragement of invention and innovation" as a purpose of trade secret protection). *See also* Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 69 (1999) (suggesting that these two justifications are "embarrassingly inadequate."). Chiappetta suggests, by examining misappropriation separately for breach of duty and for bad acts, that a more reasoned justification rests on the dual aims of leveraging holder-controlled information to achieve its greater economic exploitation and of maintaining public order and commercial privacy. *See id.* at 73.

142. *See* 18 U.S.C. § 1839(3) (1996) (providing protection that includes financial and economic information, among other types of trade secrets).

143. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 487 (1974); *see also* 1 JAGER, *supra* note 33, § 1.05 (trade secret protection also serves the function of protecting those inventions that are not novel enough to be granted patent protection, but are too utilitarian to receive copyright protection).

144. *See supra* note 65 and accompanying text. Though it has previously chosen not to do so, Congress probably could provide civil trade secret protection under their interstate commerce power. *See supra* note 64 (discussing the history of federal trademark protection).

145. *See* 1 JAGER, *supra* note 33, § 3.05[1] (reporting that, as of 1999, 44 states and the District of Columbia have adopted some form of the UTSA).

146. *See* RESTATEMENT OF TORTS § 757 (1934). The subject was not included in the Restatement (Second) of Torts because of a belief that misappropriation of trade secrets no longer belonged in the Restatement of Torts. *See* 2 JAGER, *supra* note 33, § NY.01 (discussing the history of Restatement coverage of trade secrets). Trade secrets are now covered in the Restatement (Third) of Unfair Competition. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (1995).

147. *See, e.g.*, Softel, Inc. v. Dragon Med. & Scientific Communications, Inc., 118 F.3d 955, 968 (2d Cir. 1997) ("New York generally looks to Section 757 of the First Restatement of Torts for its definition of a trade secret."); Sweetzel Inc. v. Hawk Hill Cookies Inc., 39

Under a typical scheme of trade secret protection, a trade secret could be "any formula, pattern, device, or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[148] Trade secrets frequently overlap with the protections conveyed by a patent or copyright.[149] In the case of a patent, the application may disclose the design and construction of the machine without including details, such as machining tolerances, that the applicant considers trade secrets.[150]

In order to maintain protection for the trade secret, the holder of the secret must take action to protect it from public disclosure.[151] Typical protective actions may include confidentiality clauses in employment contracts,[152] or the erection of privacy fences.[153]

Depending upon the view of the states, liability for misappropriation of a trade secret may arise either from the secret's nature as property or from the confidential nature of the relationship

---

U.S.P.Q.2d 1258, 1267 (E.D. Pa. 1995) (noting that Pennsylvania courts use the trade secret definition provided in RESTATEMENT OF TORTS § 757, comment b (1939)); Rohm & Haas Co. v. Adco Chem. Co., 689 F.2d 424, 431 (3d Cir. 1982) (noting that both "New Jersey and Pennsylvania have adopted the definition of trade secrets provided in the Restatement of Torts"); Baker v. Battershell, No. CV A 86-1895, 1986 WL 7602 (Tenn. Ct. App. July 9, 1986); Sun Dial Corp. v. Rideout, 108 A.2d 442, 445 (N.J. 1954).

148. Forest Labs., Inc. v. Pillsbury Co., 452 F.2d 621, 623 (7th Cir. 1971) (quoting RESTATEMENT OF TORTS § 757 cmt. b (1934)).

149. *See* 1 DRATLER, *supra* note 48, § 1.05[2] (stressing the importance of drafting licensing agreements to cover all necessary types of intellectual property).

150. *See generally* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974) (determining that states can provide trade secret protection on patentable items); *see also* 2 JAGER, *supra* note 33, § 10.01[3] (examining several cases where trade secrets were allowed to coexist with patents in the same machine). The patentee is, however, required to disclose the "best mode" of designing the patented item. *See* 35 U.S.C. § 112 (1998). If the information withheld from the application under the guise of a trade secret is determined to be part of the "best mode," failure to disclose it may result in the patent being invalidated. *See, e.g.*, Christianson v. Colt Indus. Operating Corp., 609 F. Supp. 1174, 1184 (C.D. Ill. 1985) (ordering Colt to disgorge all of its trade secret information relating to the interchangeability of M16 parts because they were not properly disclosed in the patent application), *rev'd*, 822 F.2d 1544 (Fed. Cir. 1987) (ruling that the patent application applied only to the rifle, not to its mass-production), *vacated by* 486 U.S. 800 (1998) (vacated on jurisdictional grounds). On appeal, the Seventh Circuit adopted the Federal Circuit's reasoning. *See* Christianson v. Colt Indus. Operating Corp., 10 U.S.P.Q.2d 1352 (7th Cir. 1989).

151. *See Pillsbury*, 452 F.2d at 624 (reviewing the factors for determining the existence of a trade secret).

152. *See* Emery Indus., Inc. v. Cottier, 202 U.S.P.Q. (BNA) 829, 836 (S.D. Oh. 1978) (balancing the interests of employer and employee to determine the enforceability of a noncompete agreement in an employment contract).

153. *See* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970) (holding that a company need not take extraordinary measures, such as roofing a construction site, to protect the secrecy of trade secrets).

between the owner and the accused.[154] Though the distinction between the theoretical bases for trade secret protection often makes little difference,[155] the theory on which the protection is based sometimes affects the outcome.[156] The majority of states protect trade secrets based on a breach of confidentiality.[157] In states that follow the confidential relationship theory, federal courts have refused to grant relief for trade secret claims based on a property theory.[158] Reliance on a breach of confidentiality also may be important to a case because of differences in the statutes of limitations and in the likelihood of receiving punitive damages.[159]

---

154. *Compare* Anaconda Co. v. Metric Tool & Die Co., 485 F. Supp. 410, 426 (D. Pa. 1980) (following the property view) *with Pillsbury*, 452 F.2d at 626 (holding that the sale of a company's subsidiary created a confidential relationship with the purchaser from which trade secret protection could arise). The confidential relationship view of trade secrets can be traced to the Roman Empire's desire to prevent citizens from obtaining confidential information through another's slaves. *See* 1 JAGER, *supra* note 33, § 1.03 (explaining the crime of "*actio seri corrupti*" or "corrupting a slave").

155. *See* 1 JAGER, *supra* note 33, § 4.01[3] (noting the willingness to combine the various trade secret theories and characterizing these distinctions as "academic and practically meaningless").

156. *See* Rohm & Haas Co. v. Adco Chem. Co., 689 F.2d 424, 430 (3d Cir. 1982) (noting that New Jersey, a confidential relationship state, and Pennsylvania, a property state, require different "supplemental elements" for a trade secrets claim).

157. *See* 1 JAGER, *supra* note 33, § 4.01[2].

158. *See, e.g.*, Winston Research Corp. v. Minnesota Mining & Mfg. Co., 350 F.2d 134, 138 (9th Cir. 1965) (citing Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964), as finding that patent policy precluded recognition of an interest in secret industrial information absent a confidential relationship); Parks v. Int'l Harvester Co., 218 U.S.P.Q. 189, 190 (N.D. Ill. 1982) (holding misappropriation to require a confidential relationship because it did not involve tangible property).

159. *See* 1 JAGER, *supra* note 33, § 4.01[2]. On the other hand, since a breach of confidentiality is a tort claim, trade secret cases based on this theory will not be sustainable against the United States. *See id.*, § 4.01[2] (noting that the United States has not waived its sovereign immunity with respect to torts). Basing the claim on a property theory of trade secrets, however, may elevate the action to a governmental taking under the Fifth Amendment. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1013 (1984) (holding EPA regulations requiring a company to disclose trade secret information to the government violated the company's due process rights); Lariscey v. United States, 949 F.2d 1137, 1145 (Fed. Cir. 1991) (requiring the government to compensate an inmate for requiring him to disclose his Kevlar cutting system to the government contractor where the inmate had secretly designed the system of his own initiative and on his own time), *aff'd en banc*, 981 F.2d 1244 (Fed Cir. 1992). Despite the advantages in a suit brought against the United States, it may be more difficult to win a trade secret claim in a state that bases its law on a property theory. *See, e.g.*, Anaconda Co. v. Metric Tool & Die Co., 485 F. Supp. 410, 426 (D. Pa. 1980) (holding that, in light of the Pennsylvania Supreme Court's rejection of a confidential relationship theory, the plaintiff must show an adverse use of the trade secret beyond the violation of a confidential relationship). Finally, states differ in the availability of criminal sanctions for trade secret theft. *See* Ruhl, *supra* note 50, at 788–802 (examining the differences between, and limitations of, state trade secret crimes and noting that only thirty states provide criminal sanctions for trade secret theft).

The trade secret law of all states allows for reverse engineering.[160] Seven states provide a specific exception for reverse engineering in their trade secret statute.[161] The states that do not make such an exception and that have adopted a version of the UTSA without commenting on reverse engineering can be presumed to have adopted the view of the drafters that reverse engineering was acceptable.[162] Finally, even those states that protect trade secrets following the Restatement can be expected to allow reverse engineering.[163]

Since the value of a trade secret lies in its owner's ability to maintain its secrecy, care must be taken in disclosing products that contain trade secrets.[164] Trade secret protection only protects the trade secret from a taking or "misappropriation."[165] Competing parties, however, may both own the same trade secret information where it was independently developed through legitimate means.[166] Examining information or products that are publicly available is considered legitimate.[167]

For example, a company may freely design competing products from information that was disclosed in a government bid process or that is observable from sales literature or photographs in annual reports.[168] A

160. *See, e.g.*, E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015–16 (5th Cir. 1970) (noting that Texas law specifically allowed the use of trade secret information that was obtained through reverse engineering from the final product).

161. *See* CAL. CIV. CODE ANN. § 3426.1(a) (West 1997); GA. CODE ANN. § 10-1-761(1) (2000); 765 ILL. COMP. STAT. ANN. § 1065/2(a) (West 1993); N.C. GEN. STAT. ANN. § 66-152(1) (2000); OR. REV. STAT. § 646.461(1) (1999); *see also* LA. REV. STAT. ANN. § 51:1431(1) cmt. a (West 1987) (disclosing reverse engineering as an example of a proper means); WIS. STAT. ANN. § 134.90(1)(a) cmt. (West 1989) (noting the position of the national conference of commissioners on uniform state laws that reverse engineering is a proper means of acquiring a trade secret).

162. *See* UNIF. TRADE SECRETS ACT § 1, cmt., 14 U.L.A. 438 (1990) (premising their approval of reverse engineering on the assumption that the item that was reverse engineered was acquired by "fair and honest means").

163. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995) (stating that "analysis of publicly available products or information [is] not [an] improper means of acquisition").

164. *See supra* notes 139–144 and accompanying test (discussing the requirements for trade secrets).

165. *See* UNIF. TRADE SECRETS ACT § 1(2), 14 U.L.A. 438 (1990) (defining misappropriation).

166. *See, e.g.*, E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015–16 (5th Cir. 1970); *see also* Smith v. Dravo Corp., 203 F.2d 369, 374 (7th Cir. 1953) (determining that Pennsylvania law examines how the trade secret information was obtained rather than how it could have been obtained).

167. *See Dravo*, 203 F.2d at 374 (reviewing a case where the defendant claimed that it could have legally appropriated the information through examination of sales literature and products provided for public display).

168. *See, e.g.*, Secure Servs. Tech., Inc. v. Time & Space Processing, Inc., 722 F. Supp. 1354, 1359–62 (E.D. Va. 1989) (finding that plaintiff terminated its rights to trade secret

competitor also may develop its design based upon inspection of a plaintiff's products that are available for sale.[169] The competitor, however, may not obtain the information through aerial photography of a fenced construction site or through encouraging an employee to violate their employment agreement.[170] These rules are fact-specific and vary among the states.[171] Generally, though, courts will enforce trade secret protections for items that are available to the public if the trade secret was obtained through a prohibited means.[172] On the other hand, they will not do so if the trade secret was discovered through a study of publicly available information.[173] This is distinct from patent protections where, despite independent development, only one applicant can be granted a patent.[174]

Despite the acceptance of reverse engineering processes in all forms of intellectual property, it appears that the EEA may allow federal prosecution for reverse engineering of trade secrets.[175] Since the life of a trade secret depends only on the owner's ability to maintain secrecy, the effect of providing trade secret protection such that others are not allowed to reverse engineer from legally obtained products is tantamount to providing a perpetual patent on the secret.[176] While this is

---

protection of features in its secure facsimile machine when it provided the machine to the government without contract restrictions); Wheelabrator Corp. v. Fogle, 317 F. Supp. 633, 638 (W.D. La. 1970) (ruling that the company's annual report containing photographs of secret equipment divulged significant parts of the secret and illustrated a lack of "secretive intent"), *aff'd per curiam*, 438 F.2d 1226 (5th Cir. 1971); Engineered Mechanical Servs., Inc. v. Langlois, 464 So. 2d 329, 335–37 (La. App. 1984) (finding alleged trade secrets to have been disclosed in plaintiff's sales brochures).

169. *See, e.g.*, Crown Indus., Inc. v. Kawneer Co., 335 F. Supp. 749, 761 (N.D. Ill. 1971) (holding sale of product constitutes public disclosure, which terminates trade secret protection, even where the product would be destroyed through disassembly).

170. *See, e.g.*, *Christopher*, 431 F.2d at 1015 (prohibiting aerial photography); Conmar Prods. Corp. v. Universal Slide Fastener Co., 172 F.2d 150, 155 (2d Cir. 1949) (finding misappropriation based on inducing plaintiff's former employees to violate a contract the defendant knew about).

171. *See generally* 1 MILGRIM, *supra* note 66, §§ 1.05[2]&[3] (examining numerous cases).

172. *See id.*

173. *See id.*

174. *See* 35 U.S.C. § 115 (Supp. 1998) (requiring applicant to sign an oath that he or she is the "original and first inventor").

175. *See supra* note 40 and accompanying text. Almost all reverse engineering schemes involve processes such as sketching, and intermediate copying. *See supra* notes 66–78 and accompanying text (describing reverse engineering); *see also* Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 600 (9th Cir. 2000) (noting that the three methods of reverse engineering a computer program that did not include simply reading about the program required the person seeking access to engage in processes "that *necessarily* involve[] copying") (emphasis added).

176. *See* Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA &

still allowable under the commerce clause, it may be an unconstitutional effort to use the commerce clause to circumvent the constitutional requirement for time limits on patents and copyrights.[177]

III. EFFECTS OF THE PROHIBITION OF REVERSE ENGINEERING

A literal interpretation of the EEA raises several concerns. These concerns can be divided into three categories: intellectual property concerns, notice concerns, and federalism concerns. These will be addressed in turn.

A. *Intellectual Property & Reverse Engineering*

The first criticism of the EEA comes from its possible construction relative to other areas of intellectual property law.[178] Intellectual property's acceptance of reverse engineering rests on the very reasoning behind the Constitution's grant of patent powers to Congress. To the extent that the EEA contradicts this policy and prohibits reverse engineering, it may stifle intellectual activity in the public domain, overshadowing the benefits of increased protection to trade secret holders. Even if the EEA is not intended to prohibit reverse engineering, its prohibition of reverse engineering processes without a specific exception for reverse engineering can be expected to chill activities in these areas.[179]

Trade secrets can be seen as falling outside the power granted to Congress to promote the useful arts.[180] While the regulation of the trade secret theft may fall within the commerce clause,[181] this particular use of

---

ENT. L.J. 1, 16 (1998) (asserting that "[r]everse engineering is one of the most important ways in which trade secrets expire").

177. *See* Railway Labor Executives' Ass'n v. Gibbons, 455 U.S. 457 (1982) (striking down bankruptcy laws that were enacted under the commerce clause in order to avoid limitations in the constitution's bankruptcy clause); *see also* Dreyfus, *supra* note 176, at 16 n.53 (arguing that the courts are "unlikely" to allow Congress to rely on the commerce clause as a way to avoid the time limitation requirement in the patent clause). *See generally* Patry, *supra* note 19 (discussing how this argument plays out in the intellectual property field).

178. *See* Pooley et al., *supra* note 30, at 195 (reporting a conflict of the EEA's criminal sanctions with formally legitimate means of competition).

179. *See* Dreyfuss, *supra* note 176, at 37 (admonishing courts to be sensitive to interpretations that may chill activities that should be legal).

180. *See supra* notes 63–65 and accompanying text (discussing the power of Congress to regulate intellectual property).

181. *See* U.S. CONST. Art. I, § 8, cl. 3; *see also* Mossinghoff et al., *supra* note 9 (discussing the belief of Congress that, since the end of the Cold War, the intelligence units of foreign governments were being utilized to appropriate U.S. industrial secrets).

that power runs contrary to the principles underlying the Constitution's patent clause.[182] If, in fact, the EEA prohibits reverse engineering—one of the primary methods by which trade secrets expire—the effect is to create perpetual patent protection.[183] Although such practice would not offend the commerce clause,[184] it most likely would be viewed as an improper use of this clause to avoid the time limit constraint of the patent clause.[185]

Reverse engineering is a method for studying protected products in an attempt to develop a more thorough understanding of the relevant art in order to create superior products.[186] The processes of studying publicly disclosed inventions and of attempting to create superior products are the very reason for the Constitutionally created protections. Failure to allow specifically for reverse engineering in the EEA will stifle these creative efforts.[187]

By providing a disincentive to study protected products, the EEA runs contrary to the general scheme of intellectual property law.[188] Some insight may be gained by examining the legislative history to determine Congress's purpose in passing the EEA and to see the extent to which it considered the effects the EEA may have on the types of competition that are normally encouraged by intellectual property law.

1. Legislative History

Congressional debate leading to passage of the EEA centered on the growing concern over industrial espionage following the end of the Cold War.[189] Given the United States' position in the international economy, Congress became aware that even friendly nations were

182. *See supra* notes 139–43 and accompanying text (discussing the purposes of trade secret protection versus patent protection).

183. *See supra* note 176 and accompanying text.

184. *See supra* note 64.

185. *See supra* note 179 and accompanying text.

186. *See supra* notes 69 and accompanying text (discussing the reasoning of the Court in *Bonito*).

187. *See* Pooley et al., *supra* note 30, at 195.

188. *See id.*

189. *See* Cohen, *supra* note 4, at S377-04 (introducing the EEA); 142 CONG. REC. S740 (daily ed. Feb. 1, 1996) (statement of Sen. Kohl) [hereinafter *Kohl-2*] (sponsoring the bill and reporting that at least fifty-seven nations were attempting to obtain advanced technologies owned by American companies).

potential foes,[190] and became preoccupied with the growing role economic strength played in national security.[191]

Because of heightened concern over economic espionage, the debate on the floor of both houses of Congress focused almost exclusively on the damage economic espionage inflicted on American industry.[192] Concern over discouraging legitimate practices was briefly mentioned,[193] and, being of secondary importance, was quickly brushed aside.[194] The bill and its prior drafts were handled in the Senate by the Select Committee on Intelligence, and the Subcommittee on Terrorism, Technology, and Government Information, and in the House by the subcommittees on Crime and on Economic and Commercial Law.[195] Committee reports contained no substantive discussion of the interaction of the EEA with the goals of intellectual property law.[196]

Similarly, Congressional testimony was completely dominated by witnesses from industry and from the intelligence and security communities.[197] The witness lists were devoid of testimony from professors or practitioners of intellectual property law. As a result, the

190. *See Kohl-2*, *supra* note 189, at S740 (listing France, Germany, Japan, and South Korea as governments that "have systematically practiced economic espionage against American companies").

191. *See Cohen*, *supra* note 4, at S377 (noting that the governments of industrialized nations "have come to see economic competition as the new central threat to their national security"); 142 CONG. REC. H10,461 (1996) (statement of Rep. Hyde) [hereinafter *Hyde*] (opining that a nation's economic interests should be treated as "an integral part" of its security interests).

192. *See generally Cohen*, *supra* note 4; *Hyde*, *supra* note 191; *Kohl-1*, *supra* note 24; *Kohl-2*, *supra* note 189; *Specter-1*, *supra* note 1; 142 CONG. REC. S740-41 (1996) (statement of Sen. Specter) [hereinafter *Specter-2*]; 142 CONG. REC. S10,882 (1996) (statement of Sen. Grassley); 142 CONG. REC. H10,461 (1996) (statement of Schumer) [hereinafter *Schumer*]; 142 CONG. REC. H12,143 (1996) (statement of Rep. McCollum) [hereinafter *McCollum*].

193. *See McCollum*, *supra* note 192, at H12,144 (suggesting that the EEA "should not" result in prosecution for legitimate collection of economic data).

194. *See Schumer*, *supra* note 192, at H10,462 (noting concerns raised in committee and opining that the EEA was "carefully fine-tuned" to avoid criminalizing whistleblowing, reverse engineering, or the carrying away of employee general knowledge and experience).

195. *See infra* note 197.

196. *See, e.g.*, H.R. REP. NO. 104-788, at 4-8 (1996) (discussing the importance of proprietary information and the inadequacy of state civil remedies); S. REP. NO. 104-359, at 5-12 (1996) (adding reports of the increasing incidence of economic espionage and a discussion of the need for a comprehensive federal law).

197. *See Economic Espionage: Hearings Before the Subcomm. On Crime of the House Judiciary Comm.*, 104th Cong. III (1996) (witness list); *Economic Espionage: Hearings Before the Select Comm. On Intelligence and the Subcomm. On Terrorism, Tech. & Gov't Info. of the Senate Comm. On the Judiciary*, 104th Cong. III (1996) (same); *Economic Intelligence: Hearings Before the Senate Select Comm. on Intelligence*, 103rd Cong. III (1993) (same); *Threat of Foreign Econ. Espionage to U.S. Corps.: Hearings Before the Subcomm. On Econ. & Commercial Law of the House Comm. on Judiciary*, 102nd Cong. III (1992) (same).

Constitutional interest in "promoting the useful arts" was largely subsumed by industrial interests.

While some members of Congress felt that the EEA did not hamper competition through legitimate activities, the legislative history is less than clear on this point.[198] In fact, one of the EEA's sponsors felt that the inquiry should "focus on whether the accused has committed one of the prohibited acts . . . rather than whether he or she has 'reverse engineered.' "[199] With this statement Senator Kohl demonstrated his willingness to discard Supreme Court precedent, the UTSA, and the laws of all fifty states.[200] Commentators who claim that the legislative history shows that reverse engineering is not prohibited rely on a later statement by Senator Kohl:[201] he went on to opine that reverse engineering is acceptable if it can be done "without violating copyright, patent, *or this law*."[202] The shortcoming of this argument rests in its circular nature. The question is whether reverse engineering, which is accepted under all forms of intellectual property, violates the EEA. The Senator, however, finds the practice acceptable if it does not contravene the EEA's other provisions. His argument was acceptable provided that the activities involved violate neither previously existing intellectual property law nor the activities delineated in the EEA.[203] Unfortunately, most commonly practiced forms of reverse engineering involve activities, such as copying and sketching, that are prohibited by the plain text of the EEA.[204] This prohibition of practices that are accepted, or even encouraged, by intellectual property law raises concern.[205]

198. *See Schumer*, *supra* note 192 (suggesting that the EEA's definition of a trade secret and the level of intent required insured only "extraordinary theft" would be prosecuted); *McCollum*, *supra* note 192 (arguing that the requirement of "proof of intent or knowledge" would protect legitimate data collection).

199. *See Kohl-1*, *supra* note 24, at S12,212 (adopting the Managers' Statement for H.R. 3723).

200. *See supra* notes 76–78 and accompanying text (discussing the wide acceptance of reverse engineering).

201. *See, e.g.*, Arthur J. Schwab & David J. Porter, *Federal Protection of Trade Secrets: Understanding the Economic Espionage Act of 1996*, 10 No. 4 J. PROPRIETARY RTS. 2 (1998) (relying on Kohl's later statement to say "the legislative history indicated that legitimate reverse engineering is not" prohibited); Spencer Simon, *The Economic Espionage Act of 1996*, 13 BERKELEY TECH. L.J. 305, 316 (1998); Darren S. Tucker, Comment, *The Federal Government's War on Espionage*, 18 U. PA. J. INT'L ECON. L. 1109, 1143 (1997).

202. *See Kohl-1*, *supra* note 24, at S12,212–13 (adopting the manager's statement for H.R. 3723) (emphasis added).

203. *See id.* at S12,213 (giving the example of an individual determining the formula for Coca-Cola simply by tasting it).

204. *See* Pooley et al., *supra* note 30, at 195 (suggesting that decompilation of a computer code for reverse engineering would violate the EEA); *see also supra* notes 66–78 and accompanying text (discussing reverse engineering).

205. *See* Pooley et al., *supra* note 30, at 196.

For example, suppose a firm wishes to make a product that is compatible with the cartridges for stand-alone video game consoles. In the process of making this product, the company needs to test its components for compatibility. To do this, it decompiles part of the code for the operating system. In the process of decompilation, intermediate copies are made of this code that is subject to copyright protection. In a case based on these facts, courts have held that, though the intermediate copies do represent copies that may constitute copyright infringement, this decompilation process is a form of reverse engineering that is considered fair use.[206] Suppose now, that part of the code contains a trade secret: even though the product containing the code was publicly available, the code is not readily ascertainable without reverse engineering, and so the trade secret does not immediately expire when the product is sold.[207] If we focus, however, on the fact that the portion of the code including the trade secret was copied, as Senator Kohl suggests, rather than that the copying was part of a reverse engineering scheme, this action arguably violates the EEA. Therefore, though the technicians are not liable for copyright infringement because their activities are fair use under copyright law, they face the threat of a fifteen-year prison term because the EEA focuses on copying instead of reverse engineering. This is clearly the wrong result.

Of course, it is possible to argue that the EEA's "without authorization" and "easily discernable by legitimate means" clauses provide a defense in cases of reverse engineering. On the other hand, when a reverse engineering effort requires substantial time and resources to complete, it is less than clear that this is easily discernable,[208] especially in light of Senator Kohl's example of discerning Coke's secret formula simply by having "highly refined taste buds."[209] It is also less than clear

206. *See* Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 599–602 (9th Cir. 2000) (laying out the facts of the case).

207. *See*, *e.g.*, Merckle GmbH v. Johnson & Johnson, 961 F. Supp. 721, 727–34 (D.N.J. 1997) (refusing to grant summary judgement for defendant despite the fact that plaintiff's product had been marketed abroad with the formulation noted on the container); Analogic Corp. v. Data Translation, Inc., 358 N.E.2d 804, 806–07 (Mass. 1976) (continuing trade secret protection of computer peripherals after marketing because one year would be required to reverse engineer); Thermotics, Inc. v. Bat-Jac Tool Co., 541 S.W.2d 255, 257–61 (Tex. Civ. App. 1976) (holding that plans for a tool accessory retained trade secret protection even though the product could have been reverse engineered); Kubik, Inc. v. Hull, 224 N.W.2d 80, 93 (Mich. 1974) (finding that initial sales of product that could be reverse engineered did not disclose the trade secret).

208. *See*, *e.g.*, *Analogic*, 358 N.E.2d at 806–07 (noting that reverse engineering the product would take approximately a year).

209. *See supra* note 24 and accompanying text. Perhaps it is telling that the Senator chose as his example of acceptable reverse engineering the use of bare human senses to ascertain the composition of one of the worlds best kept trade secrets. *See* David Silverstein, *Will Pre-Grant*

that "without authorization" refers to legal authorization when the secret's owner includes contract provisions that expressly withhold authorization to reverse engineer.[210] Maybe the courts could even find intent to prohibit reverse engineering in the political climate in which the EEA was passed.[211] Finally, it can be argued that, since the EEA was passed between the time that two other laws expressly allowing reverse engineering were passed,[212] Congress has demonstrated that it knows how to include exemptions for reverse engineering when it so desires. Therefore, the courts may assume that the exclusion of reverse engineering language in this law but not in others is an indication that Congress intended to omit it.[213] The courts, therefore, may be reluctant to read an exception for reverse engineering into the EEA.

In the end, the best that can be said for the status of reverse engineering under the EEA is that it is ambiguous.[214] Even if it is not

---

Patent Publication Undermine United States Trade Secret Law?, 23 AIPLA Q.J. 695, 702 n.25 (1995) (noting that this formula "has defied chemical analysis for more than a century" (citing Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co., 107 F.R.D. 288, 289 (D. Del. 1985))); Julie S. Turner, *The Nonmanufacturing Patent Owner: Toward a Theory of Efficient Infringement*, 86 CAL. L. REV. 179, 190 n.45 (1998) (placing the date of invention at 1899).

210. For an example of a case where reverse engineering was restricted through contract terms, see *infra* notes 252–57.

211. *See* Mahajan, *supra* note 98, at 3329 n.272 (recalling that around this time, the U.S. was opposing a proposed exception for reverse engineering in the Japanese copyright law (citing Lawrence D. Graham & Richard O. Zerbe, Jr., *Economically Efficient Treatment of Computer Software: Reverse Engineering, Protection, and Disclosure*, 22 RUTGERS COMPUTER & TECH. L.J. 61, 69 (1996))).

212. *See supra* note 78 and accompanying text.

213. *See, e.g.*, Geier v. American Honda Motor Co., 120 S.Ct. 1913, 1934 (2000) (finding that Congress did not mean to preempt a common-law liability where it had specifically done so in an earlier section); Olmstead v. Zimring, 527 U.S. 581, 622 (1999) ("Ordinary canons of construction require that we . . . not import [a provision] into other parts of the law where Congress did not see fit."); Bates v. United States, 522 U.S. 23, 29 (1997) (refusing to read a specific intent requirement into a criminal statute based on the fact that Congress did include the requirement in another section and noting "we ordinarily resist reading words . . . into a statute that do not appear on its face"); Custis v. United States, 511 U.S. 485, 492 (1994) ("when Congress intended to authorize collateral attacks on prior convictions . . . it knew how to do so."); Russello v. United States, 464 U.S. 16, 23 (1983) ("Where Congress included particular language in one section of a statute but omits it in another section . . . it is generally presumed that Congress acts intentionally. . . ") (internal quotations omitted). Of course, these cases all involved comparisons between sections of the statute. In those cases, however, the Court stated that there was a *presumption* that Congress acted intentionally. Logically, the same argument, though not a presumption, could apply when comparing different statutes. *See* United States v. Granderson, 511 U.S. 39, 63 (1994) ("The presumption loses some of its force when the sections in question are dissimilar and scattered. . . ").

214. *See* Dennis J. Kelly & Paul R. Mastrocola, *The Economic Espionage Act of 1996*, 26 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 181, 187 (2000) ("[t]he reality, however, is that while reverse engineering is not expressly prohibited . . . neither is it expressly permitted."); Dreyfuss, *supra* note 176, at 17 n.56 (noting that, since the question is what is proper under the EEA, Senator Kohl's statements, similar statements in the House, and the EEA's phrase

prohibited, however, the law generally assumes that citizens receive notice through statutes and case law, not through congressional intent.[215] Therefore, valuable and legal reverse engineering efforts may be chilled simply by the fact that their legality is in question. Finally, even if Congress did intend to allow reverse engineering, it is less than clear that the courts will feel bound to that intent in the absence of a clear statutory exemption.[216]

2. The Effects of the EEA on Scientific Advancement

The legislative history shows that the EEA was enacted in an effort to secure the economic position of the United States.[217] It was thought that stronger trade secret protection would encourage American corporations to spend the research and development money necessary to develop new technologies.[218] This would help to ensure America's continued leadership in innovative technologies.[219]

If broadly enforced, the EEA may have the opposite effect. Through disclosure of new inventions to the public, patent law allows citizens to study and improve new inventions.[220] Reverse engineering allows the study of new inventions and the creation of technologies that continually advance the state of science.[221] Congress's failure to expressly permit reverse engineering under the EEA will discourage such practices. Moreover, scientists engaging in reverse engineering now may be subject to substantial prison terms.[222] The application of such harsh penalties as punishment for activities that promote technological advancement surely

---

"ascertainable through proper means" all beg the question); Simon, *supra* note 201, at 316 ("the EEA should be amended to explicitly exempt reverse engineering from the scope of the statute."); Pamela B. Stuart, *The Criminalization of Trade Secret Theft: The Economic Espionage Act of 1996*, 4 ILSA J. INT'L & COMP. L. 373, 380 (1998) ("It is unclear what the status of reverse engineering will be under this new statute.").

215. *See* Conroy v. Aniskoff, 507 U.S. 511, 519 (1993) (Scalia, J., concurring) ("We are governed by laws, not by the intentions of legislators.").

216. *See id.*

217. *See supra* notes 189–193 and accompanying text.

218. *See id.*

219. *See id.*

220. *See supra* notes 116–22 and accompanying text.

221. *See id.*

222. *See* 18 U.S.C. § 1831 (1996) (establishing a fifteen-year prison term for espionage benefiting a foreign party); 18 U.S.C. § 1832 (1996) (establishing a ten-year prison term for theft of trade secrets); 18 U.S.C. § 1834 (1996) (requiring forfeiture of property used in the crime). In addition, when the activities serve as the basis for another federal crime, they may lay the foundation upon which to establish a pattern of racketeering activity. *See* Cohen, *supra* note 4, at S378 (noting that the federal racketeering provisions apply to economic espionage under the EEA); Mossinghoff et al., *supra* note 9, at 365 (reporting that RICO charges based upon the EEA were filed in *United States v. Pin Yen Yang*, (citation omitted)); Gidseg et al., *supra* note 50, at 846 (reporting that RICO protection is available for trade secrets).

will have results contrary to the desires of Congress. Again, even if these harsh penalties are not actually applied to researchers engaging in reverse engineering, the possibility of such use may have unintended chilling effects.[223]

B. *Notice & Reverse Engineering*

The second criticism of the EEA is a problem of notice relative to criminal law. The EEA may be read to prohibit reverse engineering. Since reverse engineering is allowed—even encouraged—by all other forms of intellectual property protection, criminalizing reverse engineering in the context of a federal trade secret law does not provide adequate notice of what is acceptable in this area.

One of the most fundamental tenets of American criminal law is that there can be no criminal prosecution for an act unless there was fair notice of its illegality.[224] The concept of notice includes the doctrine of "void for vagueness."[225]

As of Spring 2000, eighteen prosecutions had been initiated under the EEA.[226] Only three have proceeded to trial.[227] In the first to result in a

---

223. Other authors have raised concern over the effect of the EEA on employee mobility and the subsequent economic effect. *See* Dreyfuss, *supra* note 176, at 37–40. This concern, while worthy of further attention, is beyond the scope of this article.

224. *See* HERBERT L. PACKER, THE LIMITS OF THE CRIMINAL SANCTION 79–80 (1968) (describing the notice requirement as "*the* first principle" of American criminal law); PAUL H. ROBINSON, CRIMINAL LAW § 2.2 (1997) (noting the legality requirement of American criminal jurisprudence). This requirement grew out of distaste for abuses of the criminal law suffered under the British crown, and is supported by both utilitarian and retributive theories of criminal law. *See* RICHARD G. SINGER & JOHN Q. LAFOND, CRIMINAL LAW: EXAMPLES & EXPLANATIONS 5–8 (1997) (examining the history of this rule and explaining that utilitarians consider knowledge of illegality to be essential to deterrence and that retributivists consider notice to be important to finding that the defendant chose to commit a wrong). The idea of notice of the criminal law is considered to be essential to serving the Constitution's dual purpose of protecting individual freedoms and limiting government authority. *See id.* at 7. As a result, notice has been incorporated as part of the protections of Fifth Amendment. *See* WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW § 11 (1974).

225. *See id.* § 11. The void for vagueness doctrine requires that statutes be written such that an ordinary person could reasonably determine the meaning and application of the law. *See* Kolender v. Lawson, 461 U.S. 352, 357 (1983) (outlining the requirements to avoid unconstitutional vagueness); ROBINSON, *supra* note 224, § 2.2 (1997). The doctrine also can be violated where a statute grants excessive discretion for law enforcement officials to determine what offenses are punishable. *See* Papachristou v. City of Jacksonville, 405 U.S. 156, 168–70 (1972); ROBINSON, *supra* note 224, § 2.2. Statutes that fail either of these two tests will be struck down as unconstitutionally vague. *See* LAFAVE & SCOTT, *supra* note 224, § 11 (noting that this requirement is part of the Fifth Amendment for federal laws and of the Fourteenth Amendment for state statutes).

226. *See* Chris Carr et al., *The Economic Espionage Act: Bear Trap or Mousetrap?*, 8 TEX. INTELL. PROP. L.J. 159, 180–96 (2000).

227. *See* United States v. Martin, 228 F.3d 1 (1st Cir. 2000); United States v. Hsu, 155 F.3d 189 (3d Cir. 1998); United States v. Yang, 74 F. Supp. 2d 724 (N.D. Ohio 1999).

published opinion, the EEA was constitutionally challenged for vagueness.[228] Additional notice concerns arise, however, when comparing the EEA to traditional intellectual property law.

1. Known to the Public

In *United States v. Hsu*,[229] the trial court expressed concern over the EEA's requirement that the information in question not be known by the public.[230] Specifically, the court questioned whether the statute referred to the general public or to the relevant scientific or industrial communities.[231] Scholars have interpreted *Hsu* as referring to the general public.[232] This conflicts with the generally accepted civil trade secret law and patent law, both of which require the information to be unknown to those practicing in the relevant field.[233]

---

228. *See* United States v. Hsu, 155 F.3d 189 (3d Cir. 1998). The defendants in *Hsu* challenged their prosecution under the EEA on several grounds. *See* United States v. Hsu, 982 F. Supp. 1022 (E.D. Penn. 1997) (holding that the defense of legal impossibility is not available to charges of attempted theft of trade secrets), *rev'd in part*, 155 F.3d 189 (3d Cir. 1998) (reversing the trial court's discovery order that required the government to release the alleged trade secret documents to the defense); United States v. Hsu, 185 F.R.D. 192 (E.D. Pa. 1999) (holding that temporary disclosure of voluminous, technical documents during a sting operation did not waive property rights in the trade secret and ruling that the defense was not entitled to unredacted copies of the trade secret documents in order to establish a defense of entrapment). The most recent defense raised was that the EEA is unconstitutionally vague with respect to its "generally known," and "readily ascertainable" clauses. *See* United States v. Hsu, 40 F. Supp. 2d 623, 626 (E.D. Pa. 1999) (outlining the defense arguments regarding vagueness).

In the end, the court set aside its concerns over the EEA's "vaporous terms," finding that it was required to analyze vagueness with respect to the facts of the case before it. *See id.* at 631 (concluding it had to "put aside [its] considerable disquiet about the EEA's language"). Because the defendants knew their actions were illegal, the court rejected the motion to dismiss the EEA counts because it found that a plausible argument of vagueness could not be made with respect to the specific facts of the case. *See id.* at 630–31 (quoting meetings where the agent explained to Hsu that they were " 'talking about maybe even doing something, you know, that is against the law' "). The language of the opinion, however, clearly leaves room for successful vagueness arguments in the future.

229. 40 F. Supp. 2d 623, 626 (E.D. Pa. 1999).

230. *See id.* at 630 (citing 18 U.S.C. § 1839(3)(B) (1996)) (requiring that information claimed to be a trade secret "derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public").

231. *See id.*

232. *See* 1 JAGER, *supra* note 33, § 4.01[4][b].

233. *See id.* (discussing the broader reach of the EEA); Ryko Mfg. Co. v. Nu-Star, Inc., 950 F.2d 714, 718 (Fed. Cir. 1991) (determining an invention's obviousness in light of the prior art, and the level of skill and education of those working in the industry); 35 U.S.C. § 103(a) (1994) (requiring that an invention not be obvious "to a person having ordinary skill in the [relevant] art"); Lederman, *supra* note 22, at 942 (teaching that states generally protect information that derives value from not being generally known to " 'other persons

The interpretation that the EEA refers to lack of knowledge by the general public creates a situation where criminal penalties can be imposed for copying unpatentable information when it is generally known in an industry, but not to the public. This is problematic for several reasons. First, it is well established that courts are obligated to interpret vague language in a criminal statute according to the rule of lenity.[234] According to this doctrine, the statutory language must be interpreted in the way that makes the least number of actions criminal.[235] In the case of trade secrets, interpreting "the public" to mean the scientific and industrial public is more consistent with both the UTSA and with the doctrine of leniency. If Congress intended to protect a broader range of information, it should be required to sate its intent clearly in the statute. Second, such a broad reading, if taken to its logical conclusion, effectively makes trade secret candidates of any of the scientific principles beyond those taught in the most basic physics course. It is hard to see how this would maintain an American lead in the technological industries. Of course, it can be argued that Congress could not have intended this result. Where the statute is open to such broad interpretation, however, only the discretion of the prosecutor keeps such wild cases from being brought.[236] In a case where a criminal was wanted for other charges, but his actions could fit under a "broader" interpretation of the statute, it is not unreasonable to imagine that the statute could be used as a tool for such prosecutions.[237] It is precisely

---

who can obtain economic value from [it]'"(citing DEL. CODE ANN. tit. 6, § 2001(4)(a) (Supp. 1988), tit. 11, § 857(9) (1987))).

234. *See* Castillo v. United States, 120 S. Ct. 2090, 2096 (2000) (finding that a provision providing a higher sentence for use of a machine gun in committing a crime was a new criminal element, not a sentence enhancement, because the statute was unclear and the Court was required to construe it in favor of the accused (citing Staples v. United States, 511 U.S. 600, 619 n.17 (1994))); Reno v. Koray, 515 U.S. 50, 64–65 (1995) (explaining circumstances in which the rule of lenity applies); Unites States v. Bass, 404 U.S. 336, 347–48 (1971) (discussing policies underlying the rule of lenity).

235. *See Reno*, 515 U.S. at 64–65.

236. Prosecutorial discretion does not seem to provide an attractive degree of protection. *See* Geraldine Szott Moohr, *The Federal Interest in Criminal Law*, 47 SYRACUSE L. REV. 1127, 1138–41 (1997) [hereinafter *Federal Interest*] (discussing abuses of prosecutorial discretion despite assurances from the Department of Justice that broad statutes only would be enforced in narrow circumstances). The expansion of the mail fraud statute provides a good example of this lack of protection. *See id.* at 1151–62 (describing the gradual broadening of mail fraud due to novel prosecutorial claims).

237. This type of abuse is not unheard of in America. *See, e.g.*, Christopher R. Leslie, *Creating Criminals: The Injuries Inflicted by "Unenforced" Sodomy Laws*, 35 HARV. C.R.-C.L. L. REV. 103, 108 n.31 (2000) (discussing the ways in which state sodomy laws are used for purposes other than punishing sodomy); Terry A. Maroney, *The Struggle Against Hate Crime: Movement at a Crossroads*, 73 N.Y.U. L. REV. 564, 612–16 (1998) (discussing the role that hate crime laws may play in the disproportionate representation of minorities on death row). One example of how jurisprudence is gradually being expanded to allow

this type of reliance on prosecutorial discretion that has resulted in statutes being held unconstitutional in the past.[238]

Several authors who expressed concern over the EEA's effect on activities like employee mobility have taken solace in Attorney General Janet Reno's letter to Congress, which states that any EEA prosecutions brought during the first five years of the Act's life will require her personal approval.[239] These intellectual property authors feel that this extra check will prevent the use of the EEA in marginal cases in a manner that might negatively impact the economy.[240] While they are correct that, from an intellectual property perspective, this should help ensure that the EEA does not have the consequences about which they were worried, from a criminal law perspective reliance on this statement raises concerns. The fact that Congress and commentators feel the need to rely on the Attorney General to ensure that bothersome prosecutions will not be brought should raise the specter of unconstitutional reliance on prosecutorial discretion.

Furthermore, Reno's statement, though reassuring, may not go as far as these authors had hoped. In the first reported case to be decided under the EEA, the defense argued that their prosecution had not received the appropriate level of review in the Attorney General's office.[241] The Court was quick to brush this aside as a consideration to which the court "should not give any weight."[242] It is precisely this type

---

prosecutions that used to be unimaginable is what some authors refer to as the shrinking Fourth Amendment. *See, e.g.*, Chris K. Visser, *Without a Warrant, Probable Cause, or Reasonable Suspicion: Is There Any Meaning to the Fourth Amendment While Driving a Car?*, 35 HOUS. L. REV. 1683, 1684 (1999) ("American drivers would probably be surprised by the . . . virtually limitless opportunity that infractions [of traffic laws] provide for police officers to stop motorists. Police often use minor traffic violations as a pretext to investigate individuals they suspect have committed unrelated crimes."); Robert Angell, California v. Acevedo *and the Shrinking Fourth Amendment*, 21 CAP. U. L. REV. 707 (1992).

238. *See, e.g.*, Papachristou v. City of Jacksonville, 405 U.S. 156, 168–70 (1972) (invalidating a vagrancy ordinance).

239. *See, e.g.*, Kent B. Alexander & Kristen L. Wood, *The Economic Espionage Act: Setting the Stage for a New Commercial Code of Conduct*, 15 GA. ST. U. L. REV. 907, 931 (1999); Dreyfuss, *supra* note 176, at 41; Stuart, *supra* note 214, at 381.

240. *See* Thierry Olivier Desmet, *The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?*, 22 HOUS. J. INT'L L. 93, 106 (1999) (asserting that the Justice Department's failure to follow this promise to avoid border-line cases would deeply affect the economy); J. Derek Mason et al., *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, 16 COMPUTER LAW. 14, 18 (1999) (recalling Reno's promise was given in response to concern that innocent competitors would be caught up in the Act); Lorin L. Reisner, *Transforming Trade Secret Theft Violations into Federal Crimes: The Economic Espionage Act*, 15 TOURO L. REV. 139, 151 (1998) (asserting that Reno recognized the danger of such broad discretion).

241. *See* United States v. Hsu, 40 F. Supp. 2d 623, 625 n.1 (E.D. Pa. 1999).

242. *Id.* (citing Conroy v. Aniskoff, 507 U.S. 511 (1993) (Scalia, J., concurring) (espousing the illegitimacy of legislative history and quoting Judge Harold Leventhal's

of treatment by jurists of Congressional intent that demands revision of the Act.[243]

2. Conflicts with State Laws

Notice concerns under the EEA go beyond those raised by the *Hsu* opinions. Federal law does not provide civil penalties for misappropriation of trade secrets.[244] By criminalizing trade secret misappropriation in a manner that may be inconsistent with a particular state's trade secret law, the federal government fails to provide adequate notice to the citizens of that state.[245]

The EEA's failure to allow for reverse engineering is one example of this problem.[246] For example, as previously noted, the EEA has adopted the property theory of trade secrets as the federal standard.[247] By contrast, many states follow a confidential relationship theory of trade secret protection,[248] under which trade secret protection arises because of the nature of the relationship between the parties.[249] Accordingly, trade secrets embodied in publicly disclosed items still can be protected if a confidential relationship existed at the time the defendant obtained the trade secret from the plaintiff.[250] Absent such a relationship, however,

---

description of legislative history as "the equivalent of entering a crowded cocktail party and looking over the heads of the guests for one's friends").

243. *See Conroy*, 507 U.S. 511, 519 (Scalia, J., concurring) ("We are governed by laws, not by the intentions of the legislators."); United States v. R.L.C., 503 U.S. 291, 309 (1992) (Scalia, J., concurring) ("The only thing that was authoritatively adopted *for sure* was *the text* of the enactment; the rest is *necessarily* speculation.") (joined by Justices Kennedy & Thomas); Aldridge v. Williams, 3 How. 9, 24 (1845) ("The law *as it passed* is the will of the majority of both houses, and the only mode in which that will is spoken is in the act itself. . . .") (emphasis added).

244. *See supra* note 65 and accompanying text (noting that trade secret protection is traditionally a state activity).

245. *See* Dreyfuss, *supra* note 176, at 28–29 (making this argument in terms of a citizen of a foreign country).

246. *See supra* note 145 and accompanying text (discussing the acceptance of reverse engineering by all fifty states and the District of Columbia).

247. *See* Pooley et al., *supra* note 30, at 193 (noting that the EEA does not require the existence of a confidential relationship); *see also supra* notes 154–59 and accompanying text (discussing the two theories of trade secret protection).

248. *See* Furr's Inc. v. United Specialty Adver. Co., 338 S.W.2d 762, 766 (Tex. Ct. App. 1960) (requiring that a violation of the trade secret law only occurs when information meeting the requirements of a trade secret is obtained through a breach of confidence); *see also* 1 MILGRIM, *supra* note 66, § 1.05[2] (noting that the absence or inadequacy of a contract ensuring confidentiality may destroy trade secret protection in certain circumstances); *but see* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015 (5th Cir. 1970) (implying a confidential relationship where the secret is obtained through "wrongful conduct").

249. *See, e.g.*, Mercer v. C. A. Roberts Co., 570 F.2d 1232, 1238 (5th Cir. 1978).

250. *See, e.g.*, Reading & Bates Constr. Co. v. O'Donnell, 627 S.W.2d 239, 243 (Tex. Ct. App. 1982).

trade secret protection evaporates with the public release of items from which the trade secret is discernible.[251] Arguably, the EEA continues to protect the trade secrets embodied in a product that was legally acquired without the benefit of a confidential relationship.[252] As a result, actions that are not even subject to civil penalties under some state trade secret laws will now become criminal.

3. Breach of Contract as Criminal Conduct

States that pursue trade secret protection under a confidential relationship theory sometimes offer protection that is similar to that produced by property theory. In *K&G Oil Tool & Service Co. v. G&G Fishing Tool Service*,[253] for example, K&G leased a magnetic oil field "fishing tool" to G&G.[254] The fishing tool embodied a configuration of magnets that was considered to be a trade secret and was sealed inside the device.[255] G&G violated the term of the lease agreement in which it agreed not to disassemble the tool and to allow K&G to perform any repairs of the tool.[256] The Texas Supreme Court upheld an award to K&G based on the trade secret theory.[257] In reaching its holding, the Court stated that "[t]he basis of the trade secret case is a 'breach of a contract.'"[258] This same action now would be criminal under the EEA.[259] Therefore, this situation would result in a ten-year federal prison term for what is essentially a breach of contract.[260]

K&G Oil also provides an example of the fact that the vast majority of information of interest to a business's competitors can be obtained by studying sources that are legally available to the public.[261] This is not the type of trade secret misappropriation that Congress intended to deter

---

251. *See, e.g.*, Research Equip. Co. v. C.H. Galloway & Scientific Cages, Inc., 485 S.W.2d 953, 956 (Tex. Ct. App. 1972).

252. *See* Pooley et al., *supra* note 30, at 193 (citing H.R. Rep. 104-788).

253. 314 S.W.2d 782 (Tex. 1958).

254. *See id.* at 785–86 (reporting the terms of the lease agreement).

255. *See id.* at 790.

256. *See id.* at 785–86 (finding that G&G disassembled the tool for inspection and made a competing product based upon the results of their inspection).

257. *See id.* at 787 (noting that K&G was entitled to recovery under the contract despite the fact that the internal configuration *could have been* determined through testing that did not violate the contract). The important consideration is how the information was actually obtained, rather than the possibility of obtaining the same information legally. *See id.*

258. *See id.* (citing Becher v. Contoure Labs., 279 U.S. 388 (1929)).

259. *See* 18 U.S.C. §§ 1831(a)(2), 1832(a)(2) (Supp. 1996) (providing punishment for an individual who obtains trade secret information "without authorization").

260. *See* 18 U.S.C. § 1832(a)(5) (Supp. 1996).

261. *See* SIMON & HAGAN, *supra* note 23, at 85 (suggesting that 95% of information of interest for industrial espionage is publicly available in a free society). The data obtained by G&G could have been legally obtained but for the lease prevision. *See supra* note 256 and accompanying text.

when it enacted the EEA.[262] Though Congress did not foresee this result, it is clearly possible under the EEA. Reliance on the sound judgment of law enforcement officials raises vagueness concerns.[263]

4. Expanded Breadth of Trade Secret Violations

States that attach criminal sanctions to trade secret misappropriation generally draft their statutes so that their criminal protection is narrower than civil protection.[264] As a result, activities that are permitted under civil trade secret laws are clearly outside the scope of the corresponding criminal statute. By contrast, the criminal sanctions of the EEA were enacted absent any federal civil trade secret law.[265] Congress was so concerned by the reports of increased espionage activities that it gave only cursory attention to the availability of civil sanctions.[266]

As previously noted, the EEA's definition of a trade secret is very similar to that of the UTSA, which does allow reverse engineering.[267] This naturally would lead one to believe that conduct allowed under the UTSA would avoid the criminal sanctions of the EEA. The misappropriation prohibited by the EEA, however, is "significantly broader" than that prohibited by the civil penalties of the UTSA.[268] As a result, a person investigating a product employing methods long accepted under civil trade secret law could easily run afoul of the new federal statute.

Reverse engineering is one example of such conduct. Reverse engineering is commonly allowed within civil intellectual property

262. *See* SIMON & HAGAN, *supra* note 23, at 85 (noting that the espionage activities of foreign entities typically involved misuse of position, physical theft, false documentation, computer hacking, employee subversion, and false security authorizations).

263. *See supra* note 225 (discussing the two prongs of the void for vagueness doctrine).

264. *See* Lederman, *supra* note 22, at 935 (noting that existing state criminal trade secret laws follow existing civil laws); Pooley et al., *supra* note 30, at 189.

265. *See Specter-1*, *supra* note 1, at S12,208 (suggesting that the Senate would undertake the enactment of federal civil causes of action the following year).

266. *See id.*; *see also Specter-2*, *supra* note 191, at S740–41 (noting the inadequacy of state civil remedies and of counterintelligence efforts).

267. *See supra* note 34 and accompanying text (discussing the EEA definition of trade secret).

268. Pooley et al., *supra* note 30, at 192–97 (examining the breadth of the misappropriation provisions). *Compare* UNIF. TRADE SECRET ACT § 1(1), 14 U.L.A. 437 (1990) (defining improper means of acquiring a trade secret as "includ[ing] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means"); *with* 18 U.S.C. § 1832 (1996) (criminalizing, in addition to taking and carry away, acts such as copying, duplicating, sketching, altering, delivering, or communicating protected information). In fact, only North Carolina's trade secret law seems to take the broad view of misappropriation adopted by the EEA. *See* N.C. GEN. STAT. § 66-152(1) (2000).

law.[269] In fact, the Supreme Court has stated that reverse engineering is specifically supported by the public policy underlying patent law.[270] Furthermore, federal law specifically allows reverse engineering in regard to semiconductor maskworks and interoperability studies of copyrighted works.[271] By apparently criminalizing an activity that is expressly permitted by corresponding civil laws, the federal government has failed to notify citizens of the range of acceptable behavior in that area. To address such fears, proponents of the EEA point out that "it is extremely unlikely that a United States Attorney's Office would seek to prosecute, and that the Department of Justice would approve, the criminal prosecution of an individual who could not be held liable under civil trade secrets law."[272] This naked reliance on prosecutorial discretion, however, is precisely the situation that the vagueness doctrine was created to prevent.[273] By ignoring this doctrine, the EEA has taken the weakest form of intellectual property,[274] which still is not afforded federal civil protection, and imposed the harshest penalties for its transgression.

C. *Federalism & Reverse Engineering*

Finally, the EEA raises certain federalism concerns. The EEA's apparent prohibition of reverse engineering is contrary to the trade secret law of all fifty states and the District of Columbia. Creating a federal crime of an activity that is clearly allowed by all of the states raises questions regarding the proper balance between the federal and state governments.

In recent years concern has grown regarding the increasing degree of federalization of the criminal law.[275] Such federalization is criticized

269. *See supra* note 66 and accompanying text.

270. *See supra* notes 66–78 and accompanying text (discussing the role that reverse engineering plays in advancing technology).

271. *See supra* note 134 and accompanying text.

272. Peter J. Toren, *The Economic Espionage Act of 1996*, 1998 REPRESENTING HIGH TECH. COS. B-37, B-48 [hereinafter REPRESENTING]; *see also* Jamie S. Gorelick & Harry Litman, *Prosecutorial Discretion & the Federalization Debate*, 46 HASTINGS L.J. 967, 976 (1995) (arguing that prosecutorial discretion should play "the most important role" in maintaining the appropriate federalism balance).

273. *See supra* note 225 (discussing general notice requirements).

274. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 489–90 (1974) ("Trade secret law provides far weaker protection . . . ."); Nagle Indus., Inc. v. Ford Motor Co., 173 F.R.D. 446, 454 (E.D. Mich. 1997) (quoting Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 155–56 (1989)); Vault Corp. v. Quail Software Ltd., 655 F. Supp. 750, 763 (E.D. La. 1987).

275. *Compare Federalization of Crimes: Chief Justice Rehnquist on Federalization of Crimes*, 33 PROSECUTOR 9 (1999) (reprinting portions of Chief Justice Rehnquist's 1998 Report on the Federal Judiciary where he opines that "[f]ederal courts were not created to

as tipping the constitutional balance between state and federal power wherein states are supposed to be the " 'immediate and visible guardians of life and property.' "[276] Federal criminal law was originally created to punish acts that were harmful to the federal government as an institution.[277] Utilizing its commerce clause powers, however, the federal government has passed laws that affect almost every area of American life.[278]

Under our federal system, states are viewed as arenas for experimentation in order to find the best solution to important social problems.[279] The increasing federalization of crimes that are arguably local in nature distorts this balance and results in a range of evils: from a diminution of the importance of state governments to legal inefficiencies and inadequate solutions to important problems.[280] Trade secret law is a good example of law that traditionally has been left to state experimentation.

The EEA creates a federal crime out of acts that previously were considered to be state law torts.[281] The creation of such federal crimes

---

adjudicate local crimes, no matter how sensational or heinous" and states that he has asked the House Judiciary Committee's Subcommittee on Courts and Intellectual Property to investigate the issue of the general expansion of the federal jurisdiction caused by federalizing state crimes); *and* Charles D. Bonner, *The Federalization of Crime: Too Much of a Good Thing?*, 32 U. RICH. L. REV. 905, 937 (1998) (acknowledging the value of federal involvement in criminal prosecution, but suggesting that federal intervention only should be available where states can not, or do not address a problem); *and Federal Interest*, *supra* note 236 (investigating the proper balance between federal and state interests in criminal prosecutions); *and* Gregory W. O'Reilly & Robert Drizin, United States v. Lopez*: Reinvigorating the Federal Balance by Maintaining the States' Roles As The "Immediate and Visible Guardians" of Security*, 22 J. LEGIS. 1 (1996) (opining on the disadvantages of overfederalization of crime), *with* George D. Brown, *Should Federalism Shield Corruption?—Mail Fraud, State Law and Post-Lopez Analysis*, 32 CORNELL L. REV. 225, 299 (1997) (recognizing that state enforcement of state law is optimal, but that "[i]n the short run, . . . federal enforcement may be a means to get there."); *and* Tom Stacy & Kim Dayton, *The Underfederalization of Crime*, 6 CORNELL J.L. & PUB. POL'Y 247 (1997) (arguing that the federal government is not playing an active enough role in crime prevention); *and* Gorelick & Litman, *supra* note 272, at 971 (arguing that federal jurisdiction should be broad because of the federal government's ability to "undertake a complete and efficient prosecution where a state could not."); *and* John C. Jeffries, Jr. & John Gleeson, *The Federalization of Organized Crime: Advantages of Federal Prosecution*, 46 HASTINGS L.J. 1095, 1125–26 (1995) (concluding that the advantages available to federal prosecutors indicate that combating organized crime is "precisely what they should be doing.").

276. *See* O'Reilly & Drizin, *supra* note 275, at 2 (quoting Alexander Hamilton).

277. *See id.* at 5.

278. *See id.* at 5–8 (noting the virtually unconstrained use of the commerce powers).

279. *See* United States v. Lopez, 514 U.S. 549, 581 (1995) (Kennedy, J., concurring) (recalling the purpose of the federalist system).

280. *See generally* O'Reilly & Drizin, *supra* note 275, at 8–12 (discussing the consequences of unchecked federalization of state issues).

281. *See supra* note 65 and accompanying text.

may tilt the balance of federal powers. As many trade secret violations arise out of simple breach of contract disputes[282] or overzealous business rivalry, the handling of such violations is best left to state law. Policing consensual business relationships falls well outside traditional federal powers and covers acts that barely resemble the espionage activities that Congress sought to curtail when it enacted the EEA.[283]

The EEA contains a provision purporting to avoid the preemption of state trade secret laws.[284] With respect to reverse engineering, however, the EEA apparently conflicts with the trade secret law of all fifty states.[285] Criminalizing trade secret reverse engineering effectively would preempt relevant state law. This runs contrary to Congress's stated intention. The unintended discouragement of legitimate competitive activities could result in damage to America's position of economic leadership far greater than that which the EEA was drafted to control.

Finally, it is worth noting that, prior to the EEA, criminal sanctions for violation of intellectual property rights had existed only for the most egregious forms of infringement.[286] The enactment of the EEA marked the first imposition of criminal penalties for mundane types of infringement. It is troubling that this move first occurred in the area of intellectual property that is generally considered to afford the weakest protection.[287] This type of concern has prompted some commentators to declare that "[s]omething seems to have gone awry in the intellectual property bargain."[288]

IV. PROPOSAL

Since trade secret protection traditionally has been a matter of state law, and does not require the disclosure of information upon which the Constitutional provisions for other forms of intellectual property protection are based, the EEA should be repealed and the specific acts of espionage with which Congress was concerned should be criminalized. In the alternative, the EEA should be revised.

---

282. *See supra* notes 258–63 and accompanying text (discussing the importance of contractual relationships in trade secret law).

283. *See supra* notes 1–8 and accompanying text (describing the types of activities with which Congress was concerned).

284. *See* 18 U.S.C. § 1838 (1996).

285. *See supra* notes 160–63 and accompanying text.

286. *See* 18 U.S.C. § 2319 (2000).

287. *See supra* note 274.

288. Dreyfuss, *supra* note 176, at 1 (discussing the more traditional bargain where the inventor received protection in exchange for the disclosure of the intellectual property).

A. *Amendment to Allow Reverse Engineering*

First, the EEA should be amended to conform to the standard intellectual property law regarding reverse engineering.[289] The language necessary to allow reverse engineering, and to bring the EEA into compliance with the reverse engineering policy of other intellectual property law, already has been developed by Congress as part of the Semiconductor Chip Protection Act.[290] This language should be incorporated, with minor modification, into the EEA as follows:

> § 1840. Limitation: reverse engineering
>
> (1) Notwithstanding the provisions of sections 1831 and 1832, it is not a misappropriation of a trade secret for
>
> (a) a person to copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey a lawfully obtained item containing a trade secret solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied in item; or
>
> (b) a person who performs the analysis or evaluation described in paragraph (a) to incorporate the results of such conduct in an item that is made to be distributed.[291]

Where the accused can show that the appropriation of a protected trade secret was a necessary part of a study designed to promote better understanding of the technology and to create improvements, a defense of reverse engineering should be allowed.[292] Allowing reverse engineering as a defense to prosecution under the EEA ensures that the goals of intellectual property law are promoted. Such an interpretation of the law fosters competition, while simultaneously deterring the blatant acts of wrongful appropriation that the EEA was drafted to prevent.

---

289. *See supra* notes 66–78 and accompanying text (describing the law of reverse engineering).

290. *See* 17 U.S.C. § 906 (1998).

291. Adapted from 17 U.S.C. § 906 (1998). Differences between the language of this section and that of 17 U.S.C. § 906 were created to mirror the language of the prohibited acts laid out in the EEA at 18 U.S.C. § 1832(2) and to ensure that such acts were still prohibited, regardless of purpose, where the item being reverse engineered was obtained illegally.

292. *See supra* notes 70–73 and accompanying text (outlining the test for reverse engineering).

Opponents of such an amendment will point to the increased value of confidential information and the efforts undertaken by competitors to obtain it.[293] Disallowing reverse engineering, however, elevates trade secret protections to a level rivaling patent protection and diminishes the incentive to patent.[294] Since nothing is disclosed to the public by one obtaining trade secret protection, excessive protection allows the owners to have their cake and eat it too. Intellectual property law must strike a delicate balance between the inefficiency created by encouraging companies to spend increasingly large sums of money to protect their information and the inefficiency created by requiring every new enterprise to "reinvent the wheel."[295] The decision of which inefficiency to favor affects the allocation of power and scope of individual rights within our society.[296] In terms of reverse engineering, the great weight of authority clearly rests on one side of these issues.[297] Changing this balance by disallowing reverse engineering is a far-reaching decision that should not be undertaken without consideration of the possible effect on the goals of intellectual property policy.[298]

Amending the EEA to specifically allow reverse engineering would align it with all other forms of intellectual property and the states' trade secret laws. By allowing those activities that are vital to a thorough utilization of knowledge committed to the public domain, this amendment conforms to accepted intellectual property policy and eliminates the concern that the EEA stifles the development of new scientific knowledge. This amendment also eliminates the notice concerns raised by prohibiting reverse engineering activities that are encouraged by other intellectual property law. Finally, this amendment minimizes federalism concerns by ensuring that the EEA does not conflict with state trade secret laws, which allow reverse engineering.

---

293. *See supra* notes 22–28 and accompanying text (discussing the increasing incidence of industrial espionage).

294. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989) (noting this as one of the Court's concerns).

295. *Federal Criminal Fraud*, *supra* note 53, at 730–32 (noting the value of maintaining a "vibrant public domain").

296. *See* Lederman, *supra* note 22, at 1003–04 (discussing the impact of trade secret protection on the allocation of economic power and personal rights reaching to the restriction of rights of a "pure[ly] cognitive" nature). A full discussion of these policy issues is beyond the scope of this Article, but they rest at the root of any legislation in this area.

297. *See supra* notes 76–78 and accompanying text (noting the clear acceptance of reverse engineering).

298. *See supra* notes 189–92 and accompanying text (discussing the legislative environment in which the EEA was passed).

B. *Amendment to Restrict the EEA's Scope*

Second, the EEA should be limited to actual acts of industrial espionage of the kind Congress intended to prevent.[299] To preclude prosecutions amounting to the policing of contract disputes and business relationships, the EEA should be amended to include the following language:[300]

> § 1841. Exclusion: Contract and business relationships.
>
> Notwithstanding the provisions of sections 1831 and 1832, this Act shall not be enforced so as to criminalize actions constituting a breach of contract or other business relationship. This section shall not apply where such contract or business relationship was established for the purpose of facilitating acts of misappropriation.

Many trade secret misappropriation cases arising under civil law involve the copying of legally obtained items, breaches of contracts, or failure to honor confidential relationships.[301] The types of misappropriation that prompted the drafting of the EEA are more sinister. The espionage envisioned by Congress involved thefts, illegal electronic monitoring, and falsification of documents.[302] The EEA should be limited to acts such as these, and should expressly exclude misappropriations arising from a breach of contract or from failed business relationships.[303]

---

299. *See Kohl-1*, *supra* note 30, at S12,212 (claiming that the sponsors had "carefully drafted [the EEA] to ensure that [it] can only be used in flagrant and egregious cases of information theft."); *see also* REPRESENTING, *supra* note 272, arguing that prosecutions would not proceed under the EEA against defendants who did not violate civil law because to do so would be inconsistent with Congressional intent).

300. In the alternative, § 1831 could be revised to incorporate the "misappropriation by improper means" language of the UTSA. *See supra* note 267. This approach, however, requires more extensive revision of the EEA and further would limit it by excluding acts that Congress may have intended to include.

301. *See supra* notes 254–63 and accompanying text.

302. *See supra* notes 1–8 and accompanying text (giving examples of typical economic espionage).

303. It could be said that shrink-wrap, or internet, software contracts should be treated differently because there is no face-to-face bargaining involved. These contracts, however, arise when someone buys a publicly available product. Study of publicly available goods has traditionally been considered a proper means of discovering a trade secret. *See supra* note 167 and accompanying text. Furthermore, the property owner is aware that such studying occurs in these contexts and should have either implemented protective devices or charged a price commensurate with that risk. It is especially hard to see why this type of risk should be specially protected in light of the reverse engineering provisions of the Digital Millennium Copyright Act. *See supra* note 93.

Of course, some may be concerned that an exclusion for breaches of contracts will encourage potential information thieves to enter into business relationships with the intent to misappropriate the other party's trade secrets. To be sure, this situation is reminiscent of one that prompted Congress to enact the EEA. The final sentence of the proposed revision, however, grants the courts the leeway to set aside the exclusion for cases, like the *Goldberg* and *Safar* cases, where one party's intention in entering the relationship was to steal information from an unsuspecting business partner.[304]

Punishing only the most blatant types of misappropriation fits better into a federal scheme of protection than does policing contract disputes. Such a limitation also is consistent with the UTSA and the trade secret law of the majority of states and the District of Columbia.[305] By thus

304. *See supra* notes 7–8 and accompanying text (recalling the facts of these cases where French nationals sought employment with, and stole trade secrets from, U.S. firms in exchange for avoiding military service).

305. *See* UNIF. TRADE SECRETS ACT § 1(1) (amended 1985), 14 U.L.A. 437 (1990) (defining improper means of acquiring a trade secret as "includ[ing] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means"); ALA. CODE § 8-27-2(2) (Michie 1993) (following the UTSA, but including trespass and deliberate acts taken specifically to gain access by means that "enhance normal human perception, where the trade secret owner reasonably should be able to expect privacy"); ALASKA STAT. § 45.50.940(1) (Michie 2000) (adopting the UTSA definition); ARIZ. REV. STAT. ANN. § 44-401(1) (West 2000) (same); ARK. CODE ANN. § 4-75-601(1) (Michie 1996) (same); CAL. CIV. CODE § 3426.1(a) (West 1997) (adding that reverse engineering or independent derivation alone shall not be considered improper means); COLO. REV. STAT. ANN. § 7-74-102(1) (Bradford 1986) (adopting the UTSA definition); CONN. GEN. STAT. § 35-51(a) (1999) (including searching through trash); DEL. CODE ANN. tit. 6, § 2001(1) (1999) (adopting the UTSA definition); D.C. CODE ANN. § 48-501(1) (Lexis 2000) (same); FL. STAT. ch. § 688.002(1) (2000) (same); GA. CODE ANN. § 10-1-761(1) (2000) (adding that reverse engineering of a trade secret not acquired by misappropriation or independent development shall not be considered improper means); HAW. REV. STAT. § 482B-2 (2000) (same); IDAHO CODE § 48-801(1) (Michie 1997) (adopting the UTSA definition); 765 ILL. COMP. STAT. § 1065/2(a) (West 1998) (adding that, in addition to breach of a confidential relationship, breach of any "other duty to maintain secrecy or limit use" and reverse engineering or independent development shall not be considered improper means); IND. CODE § 24-2-3-2 (1998) (adopting the UTSA definition); IOWA CODE ANN. § 550.2(1) (West 1997) (same); KAN. STAT. ANN. § 60-3320(1) (1999) (same); KY. REV. STAT. ANN. § 365.880(1) (Michie 1996) (same); LA. REV. STAT. ANN. § 51:1431(1) (West 1987) (same); ME. REV. STAT. ANN. tit. 10 § 1542(1) (West 1997) (same); MD. CODE ANN., COM. LAW II § 11-1201(b) (Lexis 2000) (same); MICH. COMP. LAWS ANN. § 445.1902(a) (West Supp. 2000) (same); MINN. STAT. § 325C.01(2) (1982) (same); MISS. CODE ANN. § 75-26-3(a) (2000) (same); MO. REV. STAT. § 417.453(1) (Supp. 1999) (same); MONT. CODE ANN. § 30-14-402(1) (1999) (adding willful breach or willful inducement of a breach of a duty to maintain secrecy; and, willful breach or willful inducement of a breach of a duty imposed by common law, statute, contract, license, protective order, or other administrative order); NEB. REV. STAT. § 87-502(1) (1999) (adopting the UTSA definition); NEV. REV. STAT. § 600A.030(1) (1999) (same); N.H. REV. STAT. ANN. § 350-B:1(I) (1995) (same); N.M STAT. ANN. § 57-3A-2(A) (Michie 2000) (same); N.D. CENT. CODE § 47-25.1-01(1) (1999) (same); OHIO REV. CODE ANN.

limiting the EEA, egregious industrial spying can be deterred without unreasonably encroaching on the states' role as the primary protector of trade secrets.

Restricting the EEA to acts arising outside normal business relationships better reflects the traditional role of the federal and state governments. Congressional purposes are served because the industrial espionage that prompted enactment of the EEA is deterred. State interests also are served because federal intervention into traditional state roles is minimized. By preserving balance, this amendment further minimizes the federalism concerns raised by the EEA.

CONCLUSION

The EEA was drafted in response to an alarming increase in the use of foreign intelligence assets to steal American business secrets. In attempting to deter these activities, however, the EEA has cut too far into accepted defenses allowed by intellectual property law. In so doing, the EEA threatens to deter part of the legitimate competition that has earned American businesses the strong technological positions for which industrial spies target them.

The EEA suffers from problems in terms of Constitutional notice, conflicts with intellectual property law, and basic principles of federalism. Narrowing the statute's scope and expressly permitting reverse engineering deters the activities the EEA was drafted to prevent, while avoiding these three problem areas. Until Congress undertakes a revision of the statute, the courts should interpret the EEA narrowly to limit it to those activities characteristic of the espionage that it was drafted to deter.

---

§ 1333.61(A) (Anderson Supp. 1999) (same); OKLA. STAT. ANN. tit. 78, § 86(1) (West 1995) (same); OR. REV. STAT. § 646.461(1) (1999) (adding that reverse engineering and independent development alone shall not be considered improper means); R.I. GEN. LAWS § 6-41-1(A) (1992) (adopting the UTSA definition); S.C. CODE ANN. § 39-8-20(1) (2000) (adding breach or inducement of a breach . . . of duties imposed by common law, statute, contract, license, protective order, or other court or administrative order); S.D. CODIFIED LAWS § 37-29-1(1) (Lexis 2000) (adopting the UTSA definition); UTAH CODE ANN. § 13-24-2(1) (Lexis 1999) (same); VT. STAT. ANN. tit. 9, § 4601(1) (Lexis Supp. 2000) (same); VA. CODE ANN. § 59.1-336 (Michie 1998) (same); WASH. REV. CODE § 19.108.010(1) (2000) (same); W. VA. CODE ANN. § 47-22-1(a) (Lexis 1999) (same); WIS. STAT. § 134.90(1)(a) (1997-98) (same).