ARE CORPORATE INFORMATION ASSETS, IN THE MIDST OF DYNAMIC TECHNOLOGICAL AND INFRASTRUCTURAL ADVANCES, BEST SECURED BY LEGAL OR SELF-HELP REMEDIES?

I. INTRODUCTION

A company's bottom line success is often linked to information assets.[1] A given technology, whether it consists of a product or a corporate infrastructure, is ultimately embodied in, supported, or described by information assets.[2] This underlying reliance on information assets causes some concern about their security.[3] There are other concerns as well. First, technology and technology standards are a constantly evolving factor.[4] Fundamental technology breakthroughs can render existing laws outdated.[5] Second, information assets represent a significant portion of the modern company's net worth.[6] Real estate and other physical capital have historically constituted the bulk of corporate wealth.[7] Internet businesses, in contrast, frequently have little or no investment in these kinds of assets.[8] Third, information assets can be stored electronically and are, therefore, relatively easy to copy and transport.[9] Fourth, information assets are often protected through trade secret and copyright law.[10] Finally, foreign legal regimes do not protect information assets as stringently as U.S. law.[11]

---

1. *See* Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109, 109 (2003).

2. *Id.*

3. *See id.*

4. *See* Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-hacking Regulatory Models*, 89 GEO. L.J. 171, 198 (2000).

5. *See* Patricia Cohen, *9/11 Law Means More Snooping? Or Maybe Less?*, N.Y. TIMES, Sept. 7, 2002, at B9. With the uncertain application of technology and surveillance laws to the Internet, civil libertarians and law enforcement officials acknowledge that those laws should be updated. *Id.*

6. Andrew Beckerman-Rodau, *Trade Secrets – The New Risks to Trade Secrets Posed by Computerization*, 28 RUTGERS COMPUTER & TECH. L.J. 227, 228 (2002).

7. *See id.*

8. *See id.*

9. *See id.* at 265–66.

10. *Id.* at 227-28.

11. Robert C. Van Arnam, *Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection*, 27 N.C. J. INT'L L. & COM. REG. 95, 116-18 (2001).

Therefore, corporations should consider whether traditional legal regimes—like trade secret law and copyright law, or alternatives like federal legislation or self-help—provide the best protection strategy for information assets. Likewise, lawmakers and policy-makers ought to consider steps to improve existing laws to allow corporations to operate and to thrive worldwide.

This Comment will look at recent threats—current and potential—to corporate information assets in the form of copyrights or trade secrets. In particular, this Comment will not involve an in-depth exploration of one particular area of intellectual property law, but will frame aspects of various legal regimes and recent case law to explore the law's effectiveness from the corporate perspective of managing technological change. Part II will discuss secret, computer-based searches of electronic information, both as part of a legitimate law enforcement operation, and as part of illegal attempts to steal trade secrets or to destroy property or infrastructure. Part II will also consider existing trade secret law, federal law, and international law designed to protect trade secrets and copyrights, such as the Economic Espionage Act.[12] Part III will discuss the circumvention of property-protection technologies inherent to digital video discs (DVDs),[13] television, and the Internet. Part III will also focus on the Digital Millennium Copyright Act (DMCA)[14] and its associated weaknesses. Finally, Part IV will analyze and suggest courses of action that corporations with valuable information assets should take to bolster existing protections for those assets, and to consider proactive measures.

II. MODERN INCARNATIONS OF TRADE SECRET THEFT

Most corporations recognize that their technology infrastructures are vulnerable to attack. Experts note that technological advances, like the Internet, have contributed to a

12. Economic Espionage Act, 18 U.S.C. § 1831 (2000).

13. RANDOM HOUSE WEBSTER'S COLLEGE DICTIONARY 409 (2d ed. 1999).

14. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

recent increase in fraud and theft reports.[15] On September 18, 2001, a computer program named Nimda invaded internet computers, causing billions of dollars in damage.[16] A recent survey of information technology professionals found that approximately half of the respondents felt that "United States businesses are at risk for a major cyber attack in the next twelve months."[17] Forty-five percent said that businesses are not prepared for such an attack.[18] However, their mindset appears to be changing: "[C]ompanies have begun to shift toward viewing security as an integrated business function and not merely the province of a 'little cult in the corner of the I.T. department.'"[19]

If companies are indeed more serious about security, what intruders should concern them and what legal resources should they consider if an attacker succeeds?

A. Federal Surveillance and Disclosure Generally

Law enforcement agencies, especially those in the federal government, present a sophisticated and, perhaps, overly-intrusive threat.[20] The government has developed powerful and controversial surveillance tools and techniques in recent years to

---

15. *See* Stephen Labaton, *Downturn and Shift in Population Feed Boom in White-Collar Crime*, N.Y. TIMES, June 2, 2002, at 1.

16. John Schwartz, *Year After 9/11, Cyberspace Door is Still Ajar*, N.Y. TIMES, Sept. 9, 2002, at C1 ("Nimda spread through Internet-connected computers around the world and caused damage that was estimated in the billions of dollars. The creator of Nimda, which attacked computers and installed 'back doors' for subsequent hacker attacks, has never been identified.").

17. *Id.*

18. *Id.*

19. *Id.* (quoting Steve Hunt, Vice-President, Giga Information Group).

20. Peg Brickley, *Cyber-Wiretap Ruling Threatens Corporate Data Security*, CORP. LEGAL TIMES, May 2002, at 58.

> For reasons of space and security, corporations have data stored in many locations, often on sites run by third-party specialists. Armed with an administrative subpoena, a banking regulator, for example, can force those third parties to hand over a client's records.
>
> Such moves are on the rise . . . and the government increasingly has been getting court orders forbidding Internet service providers or data companies from warning clients that records have been searched.

Id.

counter computer-based theft and terrorism activity.[21] A number of the surveillance activities are so aggressive that they have garnered judicial scrutiny.[22]

Besides surveillance tools, how may the government's intelligence reach expand? Agencies like the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA), which formerly had little to do with each other, now coordinate and share knowledge.[23] Extending criminal-enforcement capabilities to government entities outside of the Department of Justice, such as the Securities and Exchange Commission (SEC), has also been suggested.[24] Even companies that proactively participate and share information subject to federal requirements—such as the Freedom of Information Act[25]—may unwittingly lose valuable trade secret information.[26] The growing trend of governmental invasiveness should provoke companies to re-evaluate information and data-protection practices and to stay abreast of legal developments.[27]

1. Is Computer Surveillance Subject to the Electronic Communications Privacy Act of 1986?

A federal district court recently held in *United States v. Scarfo*[28] that use of a computer surveillance program did not constitute a wiretap under the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510.[29] In *Scarfo*, the FBI used proprietary technology, known as a key logger system (KLS), to capture a suspect's password and subsequently gain

---

21. *See* James Risen & David Johnston, *War of Secrets: Not Much Has Changed in a System that Failed*, N.Y. TIMES, Sept. 8, 2002, at 1; *see also* Schwartz, *supra* note 16.

22. Brickley, *supra* note 20.

23. Risen & Johnston, *supra* note 21.

24. Joseph Weber, *Firepower for Financial Cops*, BUS. WK., Aug. 26, 2002, at 98 ("[T]hey could use tools now denied to SEC investigators, such as wiretapping . . . . Here, it would be as if the SEC borrowed some of the power of the FBI.").

25. Freedom of Information Act, 5 U.S.C. § 552 (2000).

26. Matt Richtel, *New Economy: In an Era of Tighter Security, How Much Cyberfreedom are We Willing to Surrender?*, N.Y. TIMES, Dec. 3, 2001, at C3.

27. *See id*.

28. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

29. *Id.* at 581.

access to encrypted files.[30] The FBI, under a federal search warrant, entered Scarfo's office and attempted to access an encrypted file.[31] The FBI suspected that this file included evidence of illegal gambling and loan sharking, so they later returned with another warrant to install the KLS.[32] The KLS recorded keystrokes entered by the user onto the computer keyboard, including Scarfo's password, to the suspected file.[33] The FBI used the password to retrieve the file in question.[34]

A key question in *Scarfo* was whether the KLS technology had recorded communications while Scarfo was communicating over telephone lines, thus violating the ECPA.[35] The ECPA[36]

30. *Id.* at 574.

31. *Id.*

32. *Id.*

33. *Id*.

34. *Id.*

35. *Id.* at 581.

36. 18 U.S.C. § 2510 (2000), *amended by* 18 U.S.C.A. § 2510 (West Supp. 2003). The Act defines several critical terms:

As used in this chapter—

> (1) 'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
>
> . . . .
>
> (4) 'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;
>
> . . . .
>
> (12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce;
>
> . . . .
>
> (14) 'electronic communications system' means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of

generally provides that a wire communication may not be intercepted without a wiretap order.[37] Scarfo's computer included a modem and an America Online® account, leading the court to believe the search may have been unlawful.[38] The court asked the government to fully describe the KLS technology, and it did as mandated by the Classified Information Procedures Act (CIPA).[39]

The court found that the KLS technology did not intercept

> such communications;
>
> . . . .
>
> (17) 'electronic storage' means—(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;
>
> . . . .
>
> (19) 'foreign intelligence information', for purposes of section 2517(6) of this title, means—(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—(i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States;
>
> . . . .
>
> (21) 'computer trespasser'—(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

Id.

37. 18 U.S.C. §§ 2510-11.

38. *Scarfo*, 180 F. Supp. 2d at 574-75.

39. *Id.* at 575 (citing the Classified Information Procedures Act, 18 U.S.C., App. III, §§ 1-16) [hereinafter CIPA]. The government filed an *ex parte, in camera* motion to allow the court to view the classified KLS, following the CIPA regulations. *Id*.

any wire communications as defined under the ECPA.[40] The court reasoned that the FBI "configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted in real time via the communication ports,"[41] and therefore the KLS did not intercept wire communications.[42]

2. Key Logger Systems and Similar Technologies

One outcome from *Scarfo* is that the government, using KLS, can secretly gather encrypted computer data on the basis of a warrant rather than a court order.[43] While that conclusion is troublesome to privacy advocates,[44] there are other more controversial programs at the government's disposal, including: Carnivore, Magic Lantern, and Echelon.[45]

---

40. *Id.* at 581.

41. *Id.* at 581-82. An FBI affidavit further stated:

> The default status of the keystroke component was set so that, on entry, a keystroke was normally *not* recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

Id. at 582.

> Judge Politan continued: "Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated . . . . Since Scarfo's computer possessed no other means of communicating with another computer . . . the KLS did not intercept any wire communications."

Id.

42. *Id.* at 581.

43. Brickley, *supra* note 20.

44. *See id.*

45. Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J.L. & TECH. 257, 274-77 (2002); *see also* James Bamford, *Big Brother: The Eavesdroppers: What Big Ears You Have*, GUARDIAN (London), Sept. 14, 2002, at 6 (describing the Echelon network).

a. Carnivore

Carnivore, developed by the FBI, has been referred to as a "communications traffic analyzer."[46] Carnivore is used to scan e-mail messages within a stream of information.[47] The program includes a filter that captures information based on the desired text, an e-mail address, or messages from a computer.[48] Even though a message may be encrypted, the sender's and recipient's e-mail addresses are still accessible.[49] The FBI states that Carnivore's use has been of a limited nature,[50] and access to the program has been carefully guarded.[51]

b. Magic Lantern

An FBI program that could have a greater impact on surveillance is Magic Lantern.[52] Magic Lantern is similar to KLS in that it can retrieve passwords used to break encryption schemes.[53] Whereas the KLS requires physical access to the suspect's computer,[54] Magic Lantern is installed over the Internet.[55] The program is installed by "exploiting some of the same weaknesses in popular commercial software that allow hackers to break into computers."[56]

c. Echelon

Echelon, managed in part by the U.S. National Security Agency and by other foreign governments, collects enormous amounts of messages and conversations traveling to and from telecommunications satellites.[57] The Echelon network

46. Etzioni, *supra* note 45, at 275.

47. *Id.* at 274.

48. *Id.* at 274-75.

49. *Id.* at 275.

50. *Id.*

51. *Id.*

52. *See id.* at 276-77.

53. *Id.* at 277.

54. Ted Bridis, *FBI Is Building a 'Magic Lantern'; Software Would Allow Agency to Monitor Computer Use*, WASH. POST, Nov. 23, 2001, at A15.

55. *Id*.

56. *Id*.

57. Bamford, *supra* note 45, at 6 (noting that the United States is partnered

purportedly intercepts millions of calls per half-hour, and stores them in a NSA facility with a capacity of 5 trillion pages of text.[58]

3. National Security and Intellectual Property

The vast capabilities of U.S. intelligence agencies have caused a great deal of domestic and international anxiety. For example, the European Parliament recently investigated whether Echelon was being used for industrial espionage.[59] The invasiveness and overall effectiveness of these tools beg the question of whether United States law adequately limits federal law enforcement organizations from sharing or divulging wire or electronic information.[60] To some extent, limits on information sharing and espionage are already mandated by federal law through the ECPA[61] and the Homeland Security Act.[62]

4. The Electronic Communications Protection Act

Section 2517, in part, governs information sharing among federal authorities,[63] while § 2515 prohibits the use of

---

with the United Kingdom, Canada, Australia, and New Zealand).

58. *Id.*

59. *Id.*

60. *See* Brickley, *supra* note 20. "[T]he biggest threat to corporate confidentiality is not law enforcement, the experts say. It is more likely a bureaucrat somewhere in the alphabet soup of regulatory agencies, who knows his or her way around the 'distributed environment' characteristic of corporate computer operations." *Id.*

61. 18 U.S.C. § 2510 (1986).

62. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (to be codified at 6 U.S.C.).

63. Authorization for disclosure and use of intercepted wire, oral, or electronic communications:

> (1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.
>
> . . . .
>
> (3) Any person who has received, by any means authorized by this

intercepted communications as evidence when illegally obtained.[64]

> chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.
>
> . . . .
>
> (5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter.
>
> (6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence . . . to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

18 U.S.C. § 2517 (2000), *amended by* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

64. 18 U.S.C. § 2515 (2000).

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

Id.

5. The Homeland Security Act

The recently passed Homeland Security Act authorizes the distribution of information through a technology clearinghouse[65] and information sharing.[66] In particular, the President is given broad authority to direct the sharing of information between a federal agency and federal, state, or local personnel.[67] Although the authority granted by this act is broad, the information in question must generally relate to terrorist activity or to a terrorist group.[68]

B. Private Surveillance and Trade Secret Theft

The cost of confidential business information stolen from Fortune 1000 companies has been estimated to be as high as $100 billion per year, a great deal of which results from the activities of foreign governments.[69] The attitude among some foreign competitors is that stealing information from leading U.S. companies allows them to compete on a more level playing field.[70] Foreign governments generally use their existing political and military contacts to legitimately access confidential information, although for illegitimate purposes.[71] Moreover, the end of the Cold War has given foreign intelligence agencies an

---

65. 6 U.S.C.A. § 193 (West Supp. 2003).

66. 6 U.S.C.A. § 482.

67. 6 U.S.C.A. § 482 ("The President shall prescribe and implement procedures under which relevant Federal agencies—(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel.").

68. *See* 6 U.S.C.A. § 482.

69. Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25, 26 (2001); s*ee also* Neil King, Jr. & Jess Bravin, *Call it Mission Impossible Inc.—Corporate-Spying Firms Thrive*, WALL ST. J., July 3, 2000, at B1; Alan Farnham, *How Safe Are Your Secrets?*, FORTUNE, Sept. 8, 1997, at 114. The FBI stated in 1996 that twenty-three foreign governments are stealing proprietary information from U.S. corporations at a cost of about $24 billion per year. *Id*. Countries engaged extensively in espionage activities against U.S. companies include: France, Israel, Russia, China, Iran, Cuba, the Netherlands, Belgium, Germany, Japan, Canada, India, and several Scandinavian countries. Carr & Gorman, *supra*, at 27.

70. Steve Sozio & Dave Drab, *Economic Espionage in the New Millennium*, FED. LAW., May 2001, at 24, 25.

71. *Id*.

opportunity to ply their trade in non-military endeavors.[72] Former FBI Director Louis J. Freeh indicated that eight foreign countries have been "extremely active" in using bribery, theft, and other techniques to provide trade secrets to domestic companies.[73] At one point, the FBI was investigating more than 800 cases of economic espionage.[74]

Other factors pertaining to economic espionage include the advancement of sophisticated, yet inexpensive, surveillance equipment, such as digital audio and video recorders.[75] Furthermore, company insiders can play a significant role in espionage activities; eighteen economic espionage cases prosecuted under § 1832 involved insiders.[76] Also, a recent study showed that disgruntled employees were the most likely source of an attack on a corporate computer system.[77]

C. Losing Trade Secrets Via the Internet

1. Documents on the Internet and the Prior Restraint Doctrine

In *Ford Motor Co. v. Lane*,[78] a federal court upheld First Amendment rights over trade secret rights based on the doctrine of prior restraint.[79] In *Lane*, a student published sensitive trade secret information concerning Ford's business on his personal website.[80] The student received information, some of it from Ford

72. *Id*.

73. King & Bravin, *supra* note 69 ("The French are considered the most aggressive in this regard . . . .").

74. Sozio & Drab, *supra* note 70, at 25.

75. *Id*. at 26-27.

76. *Id*. at 27.

77. *Id*.

78. Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999).

79. *Id*. at 753. The prior restraint doctrine was promulgated as early as the case of *Near v. Minnesota*, 283 U.S. 697 (1931). *Lane*, 67 F. Supp. 2d at 751. In *Near*, the Supreme Court explained that prior restraints "may be issued only in rare and extraordinary circumstances, such as when necessary to prevent the publication of troop movements during time of war, to prevent the publication of obscene material, and to prevent the overthrow of the government." *Lane*, 67 F. Supp. 2d at 751. (citing *Near*, 283 U.S. at 716.).

80. *Lane*, 67 F. Supp. 2d at 747.

employees, including photos of confidential products, internal confidential Ford memos, and Ford blueprints.[81] Lane went so far as to threaten Ford that he would encourage employees to disclose additional sensitive information and that he would publish additional documents obtained.[82]

Ford successfully filed a motion for a temporary restraining order against Lane.[83] Ford then filed a motion for a preliminary injunction, seeking to enjoin Lane from publishing any Ford internal documentation and from publishing copyrighted materials and trademarks.[84] The court in *Lane* ultimately denied the injunction to restrain publication of Ford's trade secrets.[85]

The court's application of the prior restraint doctrine focused on a Sixth Circuit opinion in *Proctor & Gamble Co. v. Bankers Trust Co*.[86] The Sixth Circuit ruled that a prior restraint on pure speech was justified when a publication threatened an interest more fundamental than the First Amendment.[87] The *Lane* court found that Ford's case was not different enough to ignore the prior restraint doctrine, even in light of the broad scope of the Internet and the alleged extortion tactics used by Lane.[88] The court concluded that "[i]n the absence of a confidentiality agreement or fiduciary duty between the parties, Ford's commercial interest in its trade secrets and Lane's alleged improper conduct in obtaining the trade secrets are not grounds

---

81. *Id*.

82. *Id*.

83. *Id*. at 748.

84. *Id*. at 746.

85. *Id*.

86. *Id*. at 751-53 (citing Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219 (6th Cir. 1996)).

87. Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 227 (6th Cir. 1996).

88. *Ford Motor Co.*, 67 F. Supp. 2d at 753.

> [W]hile the reach and power of the Internet raises serious legal implications, nothing in our jurisprudence suggests that the First Amendment is circumscribed by the size of the publisher or his audience. . . . The more troubling aspect of this case is whether Lane utilized the power of the Internet to extort concessions or privileges from Ford . . . .

Id.

for issuing a prior restraint."[89]

2. Court Documents Containing Trade Secrets

When a member of the Church of Scientology published Church documents on the Internet, and was subsequently sued, a Virginia district court held that misappropriation of trade secret information did not occur.[90] The defendant, Lerma, obtained what the Church considered to be sensitive documents from proceedings in the Ninth Circuit.[91] Lerma proceeded to publish those documents on the Internet,[92] and sent a copy of the documents to a *Washington Post* reporter.[93] When the Religious Technology Center (RTC) discovered that Lerma disclosed the information, they informed the *Post* that the documents may have been stolen.[94] The *Post* subsequently obtained the same documents through the Ninth Circuit Court and published a story five days later, including materials from the unsealed documents.[95]

The RTC sued Lerma, Lerma's Internet provider, the *Washington Post*, and two *Post* reporters seeking injunctive relief and damages.[96] The claim for misappropriation of trade secrets required the RTC to show: "(1) that it possessed a valid trade secret, (2) that the defendant acquired its trade secret, and (3) that the defendant knew or should have known that the trade secret was acquired by improper means."[97] The key issue in the RTC case was whether the information was a valid trade secret.[98] The court noted that the documents had been in a court file for more than two years and that the documents could be

89. *Id.*
90. Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1369 (E.D. Va. 1995).
91. *Id.* at 1364.
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.* at 1365.
96. *Id.*
97. *Id.* at 1368 (citing Trandes Corp. v. Atkinson, 996 F.2d 655, 660 (4th Cir. 1993)).
98. *Id.*

obtained through the RTC directly.[99] Therefore, the documents were "in the public domain for an extensive period of time" and could not be considered trade secrets.[100] The court continued: "Of even more significance is the undisputed fact that these documents were posted on the Internet . . . ."[101] The ten days in which the documents were available on the Internet caused the court to conclude that the documents "remained potentially available to the millions of Internet users around the world."[102] The court concluded that no misappropriation of trade secret occurred, and granted summary judgment in favor of the defendant's motion.[103]

The Fourth Circuit took a slightly different view of what constitutes a trade secret.[104] In *Hoechst*, the Fourth Circuit stated that no cases pertaining to the disclosure of trade secrets in public court files hold that such disclosure automatically negates the secrecy of that information.[105] "[C]ourts . . . have regarded the unsealed filing of a document as a single, non-dispositive factor to be weighed in determining whether the document's contents remain a trade secret."[106]

Even though a few cases have rejected First Amendment challenges to trade secret injunctions, it is a rare occurrence.[107]

---

99. *Id.*

100. *Id.* (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484 (1974)).

101. *Id.*

102. *Id.* "As other courts who have dealt with similar issues have observed, 'posting works to the Internet makes them "generally known"' at least to the relevant people interested in the news group." *Id*. (citing Religious Tech. Ctr. v. Netcom On-Line Comm. Serv.'s., Inc., No. C. 95-20091, Slip op. at 30 (N.D. Cal. Sept. 22, 1995)).

103. *Id.* at 1369.

104. *See* Hoechst Diafoil Co. v. Nan Ya Plastics Corp., 174 F.3d 411, 411 (4th Cir. 1999).

105. *Id.* at 418 ("[M]ost courts and commentators have not treated the secrecy requirement as an absolute, but as a relative concept.").

106. *Id.* (citing Jackson v. Hammer, 653 N.E.2d 809 (Ill. 1995).

107. *See* Francis J. Burke, Jr., et al., *Protecting Trade Secrets in a Digital World*, *in* 1 SIXTH ANNUAL INTERNET LAW INSTITUTE 467, 540 (Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. G0-007E 2002) (discussing an example of where a court rejected a First Amendment defense: "[I]n *Conley v. DSC Communications Corp*., the court rejected a [F]irst [A]mendment overbreadth challenge to a trade secret injunction because the injunction was the only way to prevent destruction of the trade secret." (citation omitted)); David Greene, *Trade*

The Internet has placed a greater—and perhaps unreasonable—burden on the owner of trade secret rights to ensure property does not make it onto the Internet.[108]

D. United States Trade Secret Provisions

A corporation's strategy for prosecuting a misappropriation claim is growing more complicated. The legal underpinnings of trade secrets are firmly rooted in state jurisprudence, but modern federal law provides alternative remedies where espionage is involved.

1. Common Law Trade Secret and The Uniform Trade Secrets Act

The classic definition of a trade secret is "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."[109] Due to the vagueness of this definition, the Restatement suggests six factors of inquiry:

> (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[110]

In addition to the common law, many states have adopted a version of the Uniform Trade Secrets Act (UTSA).[111] The UTSA

Secrets, The First Amendment and The Challenges of The Internet Age, 23 Hastings Comm. & Ent. L.J. 537, 552 (2001) (discussing preliminary injunctions).

108. *See* Victoria A. Cundiff, *Trade Secrets and the Internet: Avoiding Avoidable Disasters,* in 1 SIXTH ANNUAL INTERNET LAW INSTITUTE, *supra* note 107, at 418.

109. RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939).

110. *Id*.

111. Robert C. Dorr & Christopher H. Munch, PROTECTING TRADE SECRETS, PATENTS, COPYRIGHTS, AND TRADEMARKS 51 (2d ed. 1995) (noting that thirty-six states

was passed by Congress in 1979 to harmonize state trade secret laws.[112] The UTSA, although not adopted in the same form by all states,[113] provides a more detailed definition of trade secrets and misappropriation than existed under common law.[114]

2. The Economic Espionage Act

Despite the existing trade secret laws, U.S. companies pushed for new federal legislation in the 1990s to provide additional deterrence against misappropriation,[115] especially through foreign espionage.[116] Additionally, the U.S. economy's growing dependence on intellectual property and the ease with which it may be copied and transmitted, contributed to the

---

had adopted the UTSA at the time the book was published).

112. Van Arnam, *supra* note 11, at 105.

113. *Id.* at 107.

114. Uniform Trade Secrets Act §§ 1(2), (4), 14 U.L.A. 437 (1985) [hereinafter UTSA].

> "Misappropriation" means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake."

UTSA § 1(2).

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

UTSA § 1(4).

115. *See* Farnham, *supra* note 69.

116. Van Arnam, *supra* note 11, at 109.

motivation for federal sanctions.[117]

The Economic Espionage Act (EEA)[118] was the first federal criminal law protecting trade secrets.[119] The EEA provides significant penalties including prison terms of up to fifteen years, and fines of up to $500,000.[120] The EEA also expands an already broad definition of trade secret law by including all types of business and financial information.[121] EEA provisions specifically address instances when foreign governments misappropriate trade secrets in order to profit from their illegitimate use, and when the trade secret owner is harmed by the misappropriation.[122]

---

117. *See id*. at 96, 100-01; Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 238 (1999).

118. 18 U.S.C. §§ 1831-1839 (2000); *see generally* Carr & Gorman, *supra* note 69, at 28 n.33 (recommending a recent article on the EEA, its background, provisions, and an analysis of some of the cases filed by the government to date under the EEA).

119. Van Arnam, *supra* note 11, at 109.

120. *Id.* at 111.

121. Farnham, *supra* note 69, at 116; *see also* Louis A. Karasik, *Under the Economic Espionage Act; Combating Economic Espionage is No Longer Limited to Civil Actions to Protect Trade Secrets*, 48 FED. LAW., Oct. 2001, at 34, 36 (2001) (defining trade secret to include all forms of financial, business, scientific, technical, economic, and engineering information).

122. 18 U.S.C. §§ 1831-32 (2000).

> (a) IN GENERAL.—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.
>
> (b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.);

§ 1831.

> (a) Whoever, with intent to convert a trade secret, that is related to

Section 1831 is directed against individuals whose acts support a foreign government, instrumentality, or agent;[123] § 1832 prohibits theft of trade secrets that have ties to interstate or foreign commerce.[124]

The expansiveness of the EEA is of significant concern to commentators.[125] The EEA is considered by some to be overly broad, because petty or innocuous activities may offend the statute.[126] However, the EEA is also criticized as being ineffective against individuals protected by diplomatic immunity.[127] Practically speaking, the EEA has limited application because it requires the harmed party to convince counsel from the U.S. attorney's office that the case warrants prosecution.[128] As of 2000, the government had brought only eighteen cases under the EEA.[129]

E. International Trade Secret Provisions

Several multilateral, intellectual property regimes in force today have some element of trade secret protection.[130] The recently adopted Trade-Related Aspects of Intellectual Property Agreement (TRIPS)[131] and North American Free Trade Agreement (NAFTA)[132] agreements each provide attractive

---

> or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly.

§ 1832.

123. Sozio & Drab, *supra* note 70, at 25.

124. *Id*.

125. *See* Farnham, *supra* note 69, at 114.

126. *Id*. at 114, 116.

127. *Id.* at 114.

128. Karasik, *supra* note 121, at 36.

129. Van Arnam, *supra* note 11, at 112.

130. *Id.* at 118-21.

131. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31, 33 I.L.M. 81 (1994) [hereinafter TRIPS Agreement].

132. North American Free Trade Agreement, Dec. 17, 1992, U.S.-Can.-Mex., 32 I.L.M. 289, chs. 1-9; 32 I.L.M. 605, chs. 10-22 [hereinafter NAFTA].

protections to the trade secret owner.[133]

1. World Intellectual Property Organization and the Paris Convention

The Paris Convention was the first international agreement on IP protection.[134] It requires signatories to extend the same protections to foreign individuals as those given to their own citizens.[135] The Paris Convention does not, however, require countries to meet specific standards of protection, thus permitting and perpetuating weak national laws.[136] The Paris Convention is administered by the World Intellectual Property Organization (WIPO).[137] WIPO is a world-wide organization with broad international membership that administers intellectual-property-related treaties and encourages cooperation among its members.[138]

2. The Trade Related Aspects of Intellectual Property Agreement

Trade-Related Aspects of Intellectual Property Rights Agreement (TRIPS), adopted in the Uruguay Round of Multilateral Trade Negotiations in 1993, contains specific trade secret protections.[139] TRIPS "protects information having commercial value, not in the 'public domain,' whose owner has taken 'reasonable steps' to maintain its secrecy."[140] TRIPS also protects trade secrets by prohibiting unfair competition.[141] One clause even allows countries to establish protections for vital socio-economic and technological interests, so long as that law is not "specifically forbidden" by the prohibitions of TRIPS.[142]

---

133. Van Arnam, *supra* note 11, at 119-21.
134. *Id.* at 118.
135. *Id.*
136. *Id.*
137. *Id.* at 120.
138. *Id.*
139. TRIPS Agreement, Preamble; Van Arnam, *supra* note 11, at 119.
140. Van Arnam, *supra* note 11, at 119; *see also* TRIPS Agreement art. 39(2).
141. Van Arnam, *supra* note 11, at 119; *see also* TRIPS Agreement art. 40.
142. Van Arnam, *supra* note 11, at 119-20; *see also* TRIPS Agreement art. 8(1).

3. The North American Free Trade Agreement

NAFTA article 1711 provides specific protection for each member country's trade secrets and stipulates that trade secret protection of parties is perpetual if the information remains secret to the general public.[143] "A misappropriation . . . is only actionable if the acquiring party knew, or was grossly negligent in failing to know that its actions were illegal . . . ."[144]

F. Can Trade Secret Protection be Expanded to Reasonably Limit the Internet's Power of Dissemination?

Several commentators have recognized the unfair position that trade secret owners occupy with respect to publication of trade secrets on the Internet.[145] Some disagreement persists as to the best resolution of internet-based trade secret publication.[146]

The Internet provides an instant, global forum for publishing sensitive material.[147] Preliminary injunctions arguably would provide reasonable temporary relief to the trade secret owner that would not unduly infringe on First Amendment rights.[148] However, the Supreme Court cautioned against using the prior restraint doctrine where its effectiveness would be questionable—especially due to concerns over jurisdictional enforceability.[149] Unfortunately, U.S. courts have jurisdictional problems with the enforcement of injunctions against foreign entities, further complicating the administration of fair remedies.[150]

---

143. NAFTA, *supra* note 132, 32 I.L.M. at 675; Van Arnam, *supra* note 11, at 121.

144. Van Arnam, *supra* note 11, at 121; *see also* NAFTA, *supra* note 132, 32 I.L.M. at 680.

145. Van Arnam, *supra* note 11, at 103-04, 121; Adam W. Johnson, *Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets*, 54 FED. COMM. L.J. 517, 536 (2002); Greene, *supra* note 107, at 559.

146. Compare Johnson, *supra* note 145, at 536, with Greene, *supra* note 107, at 558-59.

147. Greene, *supra* note 107, at 559.

148. Johnson, *supra* note 145, at 539.

149. Greene, *supra* note 107, at 559-60.

150. *Id*. at 559-60 ("[A]pplying less stringent constitutional standards will not

If trade secret rights were considered to be on an equal constitutional footing with free speech, the prior restraint doctrine would apply to their publication.[151] One could argue that trade secret rights are property rights under the Fifth Amendment, and therefore would have an equal constitutional footing.[152] Similarly, one could also argue that trade secrets provide for the progress of science and useful arts as designated in Article I of the Constitution.[153]

G. Other Means for Protecting Trade Secrets

1. Patents

Patents, like other forms of intellectual property, play an important role for modern corporations due to expanding technological innovations and the corresponding expansion of intellectual property protection.[154] Many business and legal factors determine whether patent protection will offer a strategic advantage over trade secret protection.[155] Factors weighing in the favor of trade secret protection include: term of protection; cost of protection; internal use of the technology; and required disclosure.[156] Patent protection, on the other hand, is

---

solve the problem; the information will still be available to the general public. All the trade secret holder will have done is punish the publisher.").

151. Greene, *supra* note 107, at 539 ("Trade secrets . . . do not share the advantage . . .of having a constitutional dimension and thus being arguably on somewhat equal footing with the First Amendment."); Victoria A. Cundiff, *Keeping Your Intellectual Property Off the Internet: Injunctive Relief or Self Help?*, *in* 1 SIXTH ANNUAL INTERNET LAW INSTITUTE, *supra* note 107, at 407-09(discussing the basis for trade secret rights in the Constitution).

152. Cundiff, *supra* note 151, at 408 (citing Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984)).

153. 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"); Cundiff, *supra* note 151, at 408.

154. Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal and Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371, 371-72 (2002).

155. *Id.* at 380.

156. *See id.* at 383-403. Patents have a term limit of twenty years from filing, whereas trade secrets have no definite term. *Id.* at 383. The cost of obtaining patents is

often preferred in cases where subject matter that is difficult to keep secret, subject matter that has a likelihood of being reverse engineered or independently developed, subject matter that is pioneering, and instances where high employee turnover exists.[157]

2. Trademarks and Copyrights

Trademarks and copyrights also provide significant advantages over trade-secret common law. Both trademarks and copyright regimes have a constitutional basis that provides more leverage in a battle over free speech rights.[158] Both rights can be registered with the government, providing greater evidentiary value to the property right owner.[159] Both rights also have greater longevity than patents.[160]

3. Preventive Technology at the Corporate Level

Perhaps the most effective means by which corporations can avoid trade secret misappropriation is adopting both technological and policy measures that prevent theft.[161] A large

---

often more expensive than that of trade secrets. *Id.* at 400-01. Technology designed for internal use, such as a manufacturing process, is more easily protected by trade secret than technology sold in the form of a product. *Id.* at 396. Patents require public disclosure of the invention as a condition of receiving the patent. *Id.* at 394.

157. *See id.* at 391-403.Where the subject matter is difficult to keep secret, a patent is generally preferable to a trade secret. *Id.* at 397-98. Even if the subject matter can be kept secret, a patent is preferable where the subject matter is easily reverse engineered. *Id.* at 391. Where the subject matter is pioneering, patents are given particularly broad scope. *Id.* at 397. Finally, high employee turnover increases the chance that a trade secret may be disclosed. *Id.* at 398.

158. *See* Greene, *supra* note 107, at 539 n.1 (citing U.S. CONST. art. I, § 8, cl. 8). It has to be noted while copyright has it constitutional basis in the Patent and Copyright Clause of the Constitution, trademark has its constitutional basis in the Commerce Clause. *See* J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 24:90.1 (4th ed. 2003).

159. *See* Dorr, *supra* note 111, at 98, 250.

160. *See id.* at 104, 175, 268.

161. Greene, *supra* note 107, at 561 ("[T]he appropriate response to the challenges raised by the Internet is to change our economic models, not our constitutional ones . . . . [W]e should resist reactionary changes to our fundamental constitutional principles, and look first to adjusting trade practices to reflect the reality of communications in the Internet Age."); Ari B. Good, *Trade Secrets and the New Realities of the Internet Age*, 2 MARQ. INTELL. PROP. L. REV. 51, 81-85, 92-93 (1998).

number of businesses can improve inadequate policies or lack of personnel to monitor and reduce instances of trade secret theft.[162]

4. Protecting Critical Infrastructure

Although an estimated ninety percent of the Internet's infrastructure is privately owned,[163] the United States Government has increased its role in securing information assets.[164] Attacks on web sites increased from 2,000 in 1997 to 21,000 in 2000, and the occurrence of viruses increased by twenty percent in 2000.[165] Legislation has targeted companies to provide information on hackers and cyber attacks to the general public in exchange for assurances that this information will not be disclosed.[166] The legislation requests an exemption from the Freedom of Information Act for information relating to the critical infrastructure.[167]

The critical infrastructure, also referred to as the "National Infrastructure," describes the essential systems that facilitate the core functions of society.[168] The National Infrastructure includes telecommunications—power, transportation, banking, water supply, and emergency services—each of which is dependent on computer networks to organize, coordinate, and execute functions.[169] Entities responsible for protecting the

---

162. Brickley, *supra* note 20 (quoting John Ashley, Chief Technical Officer of intelligence firm CoreFacts LLC as saying: "We find a lot of companies that just don't have any form of document retention policy in place, that don't secure the data when a key person leaves . . . ."); Schwartz, *supra* note 16 (quoting an information analyst: "In surveys conducted more than a year ago, only 30 percent of all companies said they had a person responsible for connecting security efforts with the actual risks of the business . . . . [N]ow, nearly 90 percent do.").

163. Richtel, *supra* note 26.

164. *See* Schwartz, *supra* note 16. For example, early legislation proposals sought to specify antivirus and firewall software and hardware used in government systems, while technology experts pushed for more generic security standards that would be effective as new types of threats emerge. *Id.*

165. Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383, 409 n.166 (2002).

166. Richtel, *supra* note 26.

167. *Id.*

168. Milone, *supra* note 165, at 383.

169. *Id.*

National Infrastructure include the President's Special Advisor for Cyberspace Security, the Critical Infrastructure Protection Board, the National Infrastructure Advisory Counsel, the FBI, and the Department of Homeland Security.[170]

III. COPYRIGHT CIRCUMVENTION TECHNOLOGIES

Copyrights were originally intended to protect printed matter, but today they protect many original works of authorship, such as software, photos, maps, and movies.[171] Electronic, digital works are vastly easier to copy and distribute than printed works.[172] One of the more remarkable violations of copyright protection involves DVD piracy.

A. The Dismantling of DVD Protections

Two U.S. courts recently ruled on the protections available for a proprietary DVD encryption code that has been decoded and published on the Internet.[173] The U.S. Court of Appeals in *Universal City Studios, Inc. v. Corley*, upheld a permanent injunction against posting under the DMCA.[174] Similarly, the California Supreme Court, in *DVD Copy Control Ass'n v. Bunner*, upheld a preliminary injunction against posting of the code under trade secrets law.[175]

The underlying background in both cases centers on the unauthorized distribution of DVD encryption technology.[176] With the advent of DVDs, movie studios chose not to release films in digital form until they had minimized the threat of piracy.[177] They did this by establishing the DVD as the digital medium standard and by developing an encryption scheme known as Content Scramble System (CSS).[178] CSS requires a compliant

170. *Id.* at 410.
171. Beckerman-Rodau, *supra* note 154, at 372.
172. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435-36 (2d Cir. 2001).
173. Cundiff, *supra* note 151, at 403.
174. *Corley*, 273 F.3d at 429.
175. DVD Copy Control Ass'n v. Bunner, 75 P.3d 1 (Cal. 2003).
176. *Corley*, 273 F.3d at 435-36; *Bunner*, 75 P.3d at 5-7.
177. *Corley*, 273 F.3d at 436.
178. *Id.*

DVD player—one that provides the CSS encryption algorithm and a set of "player keys"—in order to display the contents on DVDs.[179] The studios license the CSS technology to DVD manufacturers, but require that the manufacturers keep the CSS algorithm and keys confidential.[180]

Two years after the release of the first DVDs, a decryption program that allowed a user to extract the DVD contents onto a computer hard drive for further use and copying was developed and posted on the Internet.[181]

1. Protecting DVDs under the DMCA – Universal City Studios, Inc. v. Corley

In *Corley*, the defendant placed an article on his website about DeCSS, the tool developed to crack CSS.[182] After sending numerous cease-and-desist letters to Corley and others, several movie studios filed suit, seeking an injunction against the defendants for violating the anti-trafficking provisions of the DMCA.[183] The federal district court issued a preliminary injunction to enjoin the defendants from posting the DeCSS

---

179. *Id.* at 437.

> With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

Id.

180. *Id.*

181. *Id.* In 1999, Norwegian Jon Johansen and two other persons developed decryption code by reverse-engineering a licensed DVD player. *Id.* Johansen was able to extract the player keys and other information needed to decrypt the CSS. *Id.* Johansen was allegedly trying to develop a DVD player for use with the Linux operating system, which, at the time, did not support any DVD players. *Id.* Johansen wrote a decryption program that executed on Microsoft's operating system in order to decrypt the licensed DVD player. *Id.* Johansen then posted the executable code on his website. *Id.* at 438. "Within months of its appearance in executable form on the website, DeCSS was widely available on the Internet, in both object code and various forms of source code." *Id.* at 439.

182. *Id.* at 439 (Corley's article discussed how CSS was cracked and explained how DeCSS could be used to copy DVDs. The defendants also posted copies of DeCSS object and source code and added links to websites where DeCSS was located. Corley's website "was only one of hundreds of web sites that began posting DeCSS near the end of 1999.").

183. *Id.* at 439, 441.

code.[184] Following trial, the district court issued a permanent injunction to bar defendants from posting the code and from linking to other instances of DeCSS.[185] The district court held that computer code—like DeCSS—was speech within the bounds of the First Amendment, but "because the DMCA is targeting the 'functional' aspect of that speech . . . it is 'content neutral' . . . and the intermediate scrutiny of *United States v. O'Brien* . . . applies, rather than the strict scrutiny normally applied for protected speech."[186] The district court concluded that the DMCA survived intermediate scrutiny and also rejected prior restraint, over-breadth, and vagueness challenges by the defendants.[187] The injunction barred the defendants from posting the DeCSS code or "offering to the public, providing, or otherwise trafficking in DeCSS" or "knowingly linking any Internet web site operated by them to any other web site containing DeCSS."[188]

The Second Circuit Court of Appeals began their review of the First Amendment challenge against the DMCA by holding that computer code may be protected under the First Amendment.[189] The court then compared and contrasted the general scope of protection afforded to content-based and content-neutral restrictions on speech.[190] Particularly concerning

---

184. *Id.* at 441. However, the defendants continued to post links to other websites with the DeCSS code. *Id.*

185. *Id.* The trial court rejected numerous arguments from the defendant including: "that CSS is not a technological measure that 'effectively controls access to a work,'"and "that DeCSS was designed to create a Linux-platform DVD player." *Id.* at 441-42. The court further concluded that "the alleged importance of DeCSS to certain fair uses of encrypted copyrighted material was immaterial to their statutory liability." *Id.* at 442.

186. *Id.* at 442.

187. *Id*. The district court also upheld the application of DMCA to the linking of DeCSS code to Corley's website, concluding that the injunction was "highly appropriate" and that "the threat of piracy was very real . . . ." *Id.*

188. *Id.* at 443.

189. *Id.* at 449.

190. *Id.* at 450.

> As the District Court recognized, the scope of protection for speech generally depends on whether the restriction is imposed because of the content of the speech. Content-based restrictions are permissible only if they serve compelling state interests and do so by the least restrictive means available. A content-neutral restriction is

to the court was the functional nature of decryption code as compared to a blueprint or a recipe that cannot yield a functional result without human comprehension of its content, human decision-making, and human action.[191] Decryption code not only allows decryption and copying of DVD content, but also the retransmission of DVD content and DeCSS.[192] The court found that these considerations drastically altered consideration of the causal link between dissemination of computer programs and their illicit use.[193] Applying this analysis to the DMCA as a content-neutral restriction, the court concluded that the DMCA did not burden substantially more speech than was necessary to further the government's legitimate interests and held that prohibiting the posting of DeCSS did not overburden First Amendment free speech rights.[194]

2. *Protecting DVDs Under Trade Secret Law* – DVD Copy Control Ass'n v. Bunner

In *Bunner*, the California Court of Appeal ruled on a DeCSS case in which the plaintiffs sued under the state's UTSA.[195] The court of appeals construed the First Amendment to include DeCSS as pure speech rather than functional speech.[196] The

---

> permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored . . . .

Id. (citations omitted). For content-neutral restrictions, the Court then quoted the standard used to determine the appropriate scope of regulation: "that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" *Id.*

191. *Id.* at 451.

192. *Id.* at 452.

193. *Id.*

> [J]ust as the realities of what any computer code can accomplish must inform the scope of its constitutional protection, so the capacity of a decryption program like DeCSS to accomplish unauthorized—indeed, unlawful—access to materials in which the Plaintiffs have intellectual property rights must inform and limit the scope of its First Amendment protection.

Id. at 453.

194. *Id.* at 455.

195. *Bunner*, 113 Cal. Rptr. at 340.

196. *Id.* at 349. "[F]irst Amendment protection is not without limits. Obscenity,

court then rejected an argument that a trade secret claim trumped First Amendment rights.[197] The court reasoned that "[p]rotections for trade secrets, however, are not comparable to protections for copyrights with respect to the First Amendment."[198] The court pointed to the "delicate balancing of two federal constitutional protections," namely, the First Amendment and Article I, § 8, clause 8.[199]

"The UTSA, on the other hand, lacks any constitutional foundation. Consequently, a clash between the trade secrets law and the First Amendment does not involve a balancing between two constitutional interests."[200] The court then concluded that the prior restraint on pure speech through the trial court's issuance of a preliminary injunction was unconstitutional.[201]

The Court of Appeals conclusion in *Bunner* essentially followed the precedent of cases like *Religious Technology Center v. Lerma*[202] where prior restraints on free speech are seldom allowed over trade secret interests.[203]

However, the California Supreme Court recently overturned the appellate holding that the preliminary injunction did not violate the First Amendment.[204] A key conclusion in the California Supreme Court's analysis was that the injunction

---

libel . . . have long been recognized as falling outside the scope of the First Amendment because they lack any social value . . . . Although the social value of DeCSS may be questionable, it is nonetheless pure speech." *Id.* at 348-49.

197. *Id.* at 349. The Court emphasized that state trade secret laws were subject to First Amendment protections: "[T]he scope of protection for trade secrets does not override the protection offered by the First Amendment . . . . The California Legislature is free to enact laws to protect trade secrets, but these provisions must bow to the protections offered by the First Amendment." *Id.*

198. *Id.*

199. *Id.*

200. *Id.* at 349-50.

201. *Id.* at 351. "Prior restraints on pure speech are highly disfavored and presumptively unconstitutional . . . . 'In the case of a prior restraint on pure speech, the hurdle is substantially higher . . . publication must threaten an interest more fundamental than the First Amendment itself.'" *Id*.

202. *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp 1362, 1369 (E.D. Va. 1995) (holding that there was no improper act from the downloading of information off the Internet).

203. *See Bunner*, 113 Cal. Rptr. 2d at 351.

204. DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 19 (Cal. 2003).

would not be a prior restraint due to the defendant's prior unlawful conduct.[205] The court determined that the injunction was content-neutral and burdened no more speech than necessary to serve the significant government interests.[206] In particular, the court recognized the significant government interest of encouraging innovation and development.[207]

3. Keeping Up With the Johansens

The inventor of DeCSS was also criminally charged and tried in court.[208] Jon Johansen was charged in Norway with digital burglary for creating and circulating the DeCSS code online but was acquitted by the Oslo City Court.[209] Judge Irene Sogn stated: "The court finds that someone who buys a DVD film that has been legally produced has legal access to the film. Something else would apply if the film had been an illegal . . . pirate copy."[210] Sogn concluded that the prosecutors did not prove Johansen had used the program to access pirated copies of films.[211]

4. Jurisdictional Issues - Pavlovich v. Superior Court

A U.S. college student, Matthew Pavlovich, was sued by the DVD Copy Control Association in a California court for posting software on the Internet to crack DVDs.[212] The California Supreme Court overturned the trial court ruling that the plaintiff could not post the software.[213] The court's opinion was primarily focused on the issue of jurisdiction.[214] The trial court held that jurisdiction was proper "[b]ecause Pavlovich knew that

---

205. *Id*. at 18.

206. *Id*. at 18.

207. *Id*. at 13. "Like patent and copyright law, trade secret law 'prompt[s] the independent innovator to proceed with the discovery and exploitation of his invention.'" *Id*.

208. *Teen Wins Acquittal Over DVDs*, HOUS. CHRON., Jan. 8, 2003, at 3B.

209. *Id.*

210. *Id.*

211. *Id.*

212. *See* Pavlovich v. Superior Court, 58 P.3d 2, 5 (Cal. 2002).

213. *See id*. at 2-13.

214. *Id*.

posting DeCSS . . . would harm the movie and computer industries in California and because 'the reach of the Internet is also the reach of the extension of the poster's presence . . . .'"[215] However, the supreme court held that Pavlovich's knowledge that his conduct may harm California industries was not sufficient to establish jurisdiction.[216]

B. Deterring DeCSS and Similar Copyright Violations

1. The Digital Millennium Copyright Act[217]

To what extent is the DMCA an effective deterrent against electronic piracy? Some Washington officials—such as Richard Clarke, Director of Computer Network Security for President Bush, and Democratic Congressman Rick Boucher—think the DMCA is overly broad in scope.[218] Boucher has stated that the DMCA criminalizes innocent conduct and has promoted legislation legalizing Johansen's software for personal use but not for producing mass copies of DVDs.[219]

Using DeCSS as an example, which parties are affected under the DMCA? The DMCA, in § 1201(a), outlawed the circumvention of technological measures like CSS.[220] The people

---

215. *Id.* at 6.

216. *Id.* at 13.

217. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

218. Hiawatha Bray, *Upgrade Technology & Innovation; Free Software vs. Goliaths; Open-Source Movement Faces Big Adversaries*, BOSTON GLOBE, Nov. 25, 2002, at F3.

219. *Id.*

220. 17 U.S.C. § 1201(a) (2001). Section 1201(a) of the DMCA provides in pertinent part:

> Violations regarding circumvention of technological measures.—(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.
>
> . . . .
>
> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited

who post and distribute DeCSS are clearly subject to DMCA provisions.[221] With regard to Johansen, an argument can be made that his acts merely constitute reverse engineering, which is traditionally a legal practice.[222] Section 1201(f) provides for the following exemption:

> [A] person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention . . . .[223]

Such acts are allowed, provided the acts and the associated means for carrying them out do not constitute infringement.[224] One may infer from the case of *Universal City Studios, Inc. v. Reimerdes* that the court would not convict Johansen on the basis of authoring the DeCSS, where the sole purpose of CSS circumvention was to achieve interoperability.[225] However, the DMCA appears to cut against historical acceptance of reverse engineering by sanctioning only some forms of it and by further

---

> commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure . . . .

17 U.S.C. 1201(a)(1)(A), (a)(2)(A)-(C). Section 1201 further defines the act of circumventing a technological measure as "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner . . . ." § 1201(a)(3)(A).

221. *Corley*, 273 F.3d at 455-56.

222. Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1582 (2002).

223. 17 U.S.C. § 1201(f)(1).

224. *See id.*

225. John W. Hazard, Jr., 1 COPYRIGHT LAW IN BUSINESS AND PRACTICE, § 7:36 (Rev. ed. 2002) (discussing the outcome in Universal City Studios, Inc. v. Reimerdes, 104 F. Supp. 2d 334 (S.D.N.Y. 2000) and applying the court's reasoning to Johansen's case).

limiting what can be done with the results from reversing engineering.[226] Ultimately, the DMCA's broad anti-piracy restrictions will likely be relaxed.[227]

2. Alternatives

The movie industry has clearly not solved the video piracy problem through civil suits, nor have law-enforcement authorities clamped down on DVD piracy to the extent that the industry would like.[228] Jack Valenti, President of the Motion Picture Association of America (MPAA), says that videocassette piracy alone costs the industry more than $3.5 billion.[229] The MPAA also states that $2 billion to $3 billion in ticket sales and legitimate, international DVD sales are lost each year.[230]

Piracy over the Internet is a greater concern for Valenti because of the speed at which copies may be distributed.[231] Valenti, however, rejects the charge that the industry is deliberately holding back internet movie business and that "copyrighted movies are destroying digital innovation."[232] Valenti urges that the solution to eliminating piracy over the Internet is to have computers and other video players must react to instructions embedded in the film.[233] The MPAA effort to build security into electronic devices is a contentious point with computer and electronics manufacturers, but both sides are

226. Samuelson & Scotchmer, *supra* note 222, at 1630-1631.

227. *See* Universal City Studios, Inc. v. Reimerdes, 104 F. Supp. 2d 334 (S.D.N.Y. 2000); *see also* Bray, *supra* note 218.

228. Hiawatha Bray, *Pirate Enterprise Illegal DVD Copies Put Hollywood on Offensive*, BOSTON GLOBE, Jan. 9, 2003, at E1. Jack Valenti, Motion Picture Association of America President, stated that fourteen federal raids were staged in Boston in 2002, while local Boston law-enforcement had not investigated one case of DVD piracy. Valenti also commented that during the first nine months of 2002, federal authorities were involved in 1035 raids in the United States. *Id.*

229. Jack Valenti, *Movies Get Framed: Films on the Net – We'd Love It. But Not for Free*, WASH. POST, Feb. 25, 2002, at A23.

230. Bray, *supra* note 228.

231. Valenti, *supra* note 229 (noting that approximately 350,000 films are being illegally downloaded per day).

232. *Id.*

233. *Id.*

apparently discussing the issue.[234] Valenti believes that if manufacturers are not willing to develop these copyright protection measures, then congressional legislation may be required.[235]

The MPAA, however, was recently left out of a deal struck between a number of leading technology companies, represented by the Business Software Alliance, and the Recording Industry Association of America (RIAA).[236] Companies including Microsoft, IBM, and Dell agreed to provide support for anti-piracy efforts in exchange for RIAA's promise to argue against legislative requirements for locking controls in entertainment devices.[237] The deal may affect the outcome of legislation requiring that devices include copy restriction technology.[238]

C. Digital Video Recording Technology

Movie and television plaintiffs are also wrestling over the legality of digital video recording (DVR) technology as provided by ReplayTV.[239] ReplayTV provides a recording service that allows users to record television shows on a hard drive and share those recorded shows with other users, all while skipping commercials.[240] In April 2002, the movie studios and networks sued SONICBlue for producing the ReplayTV recording device, alleging copyright infringement.[241] In August, five ReplayTV owners filed a declaratory action against entertainment industry defendants to obtain a judicial ruling on the question of copyright infringement.[242]

---

234. Bray, *supra* note 228.

235. Valenti, *supra* note 229.

236. Ted Bridis, *Music, Technology Groups Agree on Copyright Plans*, ASSOCIATED PRESS NEWSWIRES, Jan. 14, 2003, *available at* WL 1/14/03 APRWIRES 03:09:00.

237. *Id.*

238. *Id.*

239. HAZARD, *supra* note 225, 2003 Supp., WL COPYLBP § 7:36.

240. *Id.*

241. *Id.* (citing Paramount Pictures Corp. v. ReplayTV, Inc., 2002 WL 1315811 (C.D. Cal. 2002)). For more information on the SONICBlue case, see http://www.siliconvalley.com/mld/siliconvalley/3186191.htm (May 2, 2002).

242. HAZARD, *supra* note 225, 2003 Supp., WL COPYLBP § 7:36; Newmark v. Turner Broadcasting Network, 226 F. Supp. 2d 1215, 1218 (C.D. Cal. 2002).

D. Internet Pop-up Advertisements

The internet company Gator Corporation is currently facing suit by several news publishers as well as United Parcel Service (UPS) for alleged copyright and trademark infringement.[243] Gator Corporation provides a free "digital wallet" service that allows users to store names, passwords, and other information for internet shopping.[244] However, the plaintiffs in *Washingtonpost.Newsweek Interactive Co. v. Gator Corp.*[245] contend that the software is a "Trojan horse" that includes a program—known as OfferCompanion—for tracking the user's internet activity and sending the information back to Gator.[246] The Gator then placed ads on the plaintiffs' websites without dealing directly with the plaintiffs.[247] The complaint alleged violations of trademark, unfair competition, trademark dilution, copyright infringement, contributory copyright infringement, misappropriation, interference with prospective economic advantage, and unjust enrichment.[248] In July 2002, the district court in Virginia granted the plaintiffs' motion for preliminary injunction.[249] UPS has filed a separate suit in United States District Court for similar violations due to pop-up ads.[250]

---

243. *Gator Faces Another Pop-up Ad Suit*, INTERNET NEWSL. (NLP IP Co., New York, N.Y.), Oct. 2002; *Judge Issues TRO Against Pop-up Ad Firm*, 9 ANDREWS INTELL. PROP. LITIG. REP. 9, Aug. 20, 2002.

244. *Copyrights: Judge Issues TRO Against Pop-up Ad Firm*, 9 ANDREWS INTELL. PROP. LITIG. REP. 9, Aug. 9, 2002.

245. Washingtonpost.Newsweek Interactive Co. v. Gator Corp., No. Civ. A.02-909-A, 2002 WL 31356645, at *1 (E.D. Va. Jul. 16, 2002).

246. *Copyrights: Judge Issues TRO Against Pop-up Ad Firm*, *supra* note 244.

> When a PC user whose computer is running OfferCompanion visits certain Web sites, Gator's computer system will launch one or more pop-up ads to be displayed directly over the content the Web site owner intends visitors to see. In turn, the complaint explains, Gator sells the addresses of plaintiffs' Web sites to companies that wish to reach targeted audiences with pop-up ads.

Id.

247. *Id.* (One example was where an ad for hotjobs.com appeared on the competing website of plaintiff Dow Jones' CareerJournal.com.).

248. *Id.*

249. *Washingtonpost.Newsweek Interactive Co.*, 2002 WL 31356645 at *1.

250. *Gator Faces Another Pop-up Suit*, *supra* note 243.

IV. PRESERVING INFORMATION ASSETS

A wide cross-section of technologies is eroding the viability of trade secret and copyright protection. The task of battling this erosion presents unique challenges to the United States judiciary and legislature as they attempt to balance existing legal and societal norms with an ever changing technological landscape.

A. Judicial Balancing of First Amendment and Information Asset Interests

The constitutional basis for protection of information assets is a fulcrum whose position is shifting. Cases such as *Corley* demonstrate that these interests may legitimately and fairly prevail over a finely delineated area of speech.[251] In *Corley*, the DMCA was found to be on equal footing with the First Amendment—a position affirmed by other courts.[252] Some believe that trade secrets "do not share the advantage, unlike their intellectual property cousins, copyright and patent, of having a constitutional dimension and thus being arguably on somewhat equal footing with the First Amendment."[253] However, the Supreme Court has held that trade secrets are property rights under the Takings Clause of the Fifth Amendment.[254] Therefore, publication of trade secret information may trigger a *Corley*-type analysis if the publisher uses a First Amendment defense.[255]

The *Corley* analysis can and should be extended to unauthorized publications of trade secrets, especially where the Internet is used as a vehicle for rapid and widespread dissemination. Such a restriction should be considered content-neutral—and therefore permissible—if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly

---

251. *See supra* Section III.A.1.

252. *See* Dallas Cowboys Cheerleaders, Inc. v. Scoreboard, 600 F.2d 1184, 1187 (5th Cir. 1979).

253. Greene, *supra* note 107, at 539.

254. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1003-04 (1984).

255. *See Corley*, 273 F.3d at 450.

tailored.[256] Hypothetically, a court should consider a number of factors in determining whether a substantial governmental interest exists, such as whether interstate commerce is involved or the degree to which the technology is already regulated.

B. Legislatively Enhance Corporate Self-help Options

Do modern companies sometimes place too much emphasis on legal remedy rather than implementing technological precautions against theft of information assets? The deal struck by the Business Software Alliance and the RIAA demonstrates a sentiment that self-help provides a better remedy for information theft, at least in the short-term, than legislation.[257] The impact of widespread, high-tech driven, information piracy on the national economy begs the question: Should government lead self-help efforts and provide some financial backing?

A strategy of intellectual-property legislative reform for long-term protection—combined with short-term support in the form of carefully crafted self-help initiatives—may be the best way for government to reasonably keep pace with developments in technology and allow corporations to be successful.

V. CONCLUSION

Corporate information assets are more vital than ever in highly competitive national and international business environments. Many of these assets—particularly trade secrets—are not being given the proper amount of legal, technological, and policy protection. The Internet has provided a vehicle for sophisticated thieves, hackers, entrepreneurs, and activists to infiltrate corporate networks and avoid hardware and software protection schemes.[258] The ineffectiveness of current measures has resulted in a rash of federal statutes that receive mixed reviews from corporate backers.[259] Some firms are beginning to realize that the dynamics and speed of technology development make self-help a more responsive approach in the

256. *See Corley*, 273 F.3d at 450.

257. Bridis, *supra* note 236; *see also* Cundiff, *supra* note 151, at 411.

258. *See supra* Section III.

259. *See supra* Sections II.D.2.—G.1, III.B.—IV.B.

near-term than legislative efforts or trips to the courthouse.[260] There is a great deal of evidence to suggest that the fifteen-year-old hackers of the future will continue to stay several steps ahead of Capitol Hill, if not corporations.[261] In that climate, it will be up to corporations to proactively forge alliances and foster standards that will close technological loop-holes in software and hardware products, while concurrently lobbying for broad but sensible long-term legal protections. At stake is not only the viability of a particular business, but the competitiveness of U.S. industry in the international market.

*Randall W. Schwartz**

260. *See infra* Section IV.B.

261. *See, e.g., FBI Arrests Teenager Suspected as Hacker of Pentagon System*, WALL ST. J., Sept. 1, 1999, at A28; John Simons, *Web of Mystery: A Hacker's Sojourn Finds Him Ensnared in an FBI Dragnet*, WALL ST. J., June 14, 1999, at A1.

* Recipient of the Porter & Hedges, L.L.P. Writing Award for an Outstanding Comment on a Corporate-Related Topic.