2004

Access Denied: Improper use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites

Christine Galbraith Davik
University of Maine School of Law, christine.davik@maine.edu

ACCESS DENIED: IMPROPER USE OF THE COMPUTER FRAUD AND ABUSE ACT TO CONTROL INFORMATION ON PUBLICLY ACCESSIBLE INTERNET WEBSITES

CHRISTINE D. GALBRAITH*

Imagine that you are walking down the sidewalk on a public street on your way to the grocery store. You notice a new produce market with a huge front display window that has a sign stating "Grand Opening: Huge Produce Sale." The advertisement lists the price per pound of various fruits and vegetables and is completely visible from the street. You copy down the prices of various items on a piece of paper you have in your wallet, intending to compare the prices advertised with those at the grocery store you normally frequent.

Have you done something wrong? Could your behavior even be categorized as criminal? Such a suggestion probably seems absurd. Nonetheless, strange as it may seem, if this same scenario were to occur within the electronic world, it is possible that you might have violated the Computer Fraud and Abuse Act.[1]

Hacking has been defined as illegally gaining access to and sometimes tampering with information in a computer system.[2] Additionally, transmitting a computer virus that corrupts and disables a computer system also constitutes hacking.[3] But does hacking include accessing and using the uncopyrightable, factual information[4] that a company has chosen to post on a publicly accessible website?[5] A num-

---

* Associate Professor of Law, University of Maine School of Law. B.S., University of Illinois; J.D., University of Illinois. Many thanks to Maureen O'Rourke, Laura Underkuffler, Colleen Khoury, Lois Lupica, Jennifer Wriggins, and Don Zillman for their insightful comments on an earlier draft of this Article. Additionally, I would like to thank the participants in both the New England Junior Faculty Exchange and the Faculty Workshop at the University of Maine School of Law for allowing me to present the arguments in this paper at an early stage of development, as well as obtain invaluable comments and thoughts.

1. 18 U.S.C. § 1030 (2000 & Supp. 2003).

2. *See* Merriam-Webster Online, *at* http://www.merriamwebster.com (last visited Jan. 21, 2004) (defining "hack" as "to gain access to a computer illegally").

3. *See* Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 849 (1999) (noting that "[i]njecting malicious code (commonly referred to as 'viruses') is another type of hacking with potentially devastating effects").

4. *See infra* Part II (distinguishing protectable and unprotectable material under copyright law).

5. The term "publicly accessible" or "publicly available" refers to websites on the World Wide Web that are openly accessible to the general public.

ber of companies have recently tried to argue—and have surprisingly succeeded—in convincing courts that it should.[6]

I. INTRODUCTION

The Internet, once used only by government agencies and universities, has quickly become an important mechanism for commerce.[7] In 1991, the first web page in the United States was posted on the World Wide Web.[8] Current estimates, however, place the number of web pages on the Internet at three billion.[9] This phenomenal rate of growth is due in large part to the utilization of the Internet as a major commercial center. Companies once relegated to the world of "bricks and mortar,"[10] have now staked out their place in cyberspace. This often includes creating a website that provides information to the public about the goods or services the company offers, as well as a means for obtaining or ordering them.[11] The free flow of information is viewed as one of the most important and defining features of the Internet,[12] leading to its nickname, the "Information Superhighway."

Unfortunately, data once unquestionably part of the public domain is now increasingly becoming subjected to private claims of ownership. In an attempt to control competition and maintain market share, companies are now seeking to prevent the utilization of the

---

6. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000) (enjoining defendant from accessing noncopyrightable information on plaintiff's website).

7. *See* Brookfield Communications, Inc. v. West Coast Entm't Corp., 174 F.3d 1036, 1044 (9th Cir. 1999) (noting that "companies are racing to stake out their place in cyberspace"); United States v. Microsoft Corp., 147 F.3d 935, 939 (D.C. Cir. 1998) (discussing the rapid growth of the World Wide Web).

8. Paul Festa, *Ten Years Ago: Switching on the World Wide Web*, CNET News.com, Dec. 10, 2001, *at* http://news.zdnet.co.uk.

9. Yuki Nogachi, *Online Search Engines Help Lift Cover of Privacy*, WASH. POST, Feb. 9, 2004, at A1.

10. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1065 n.11 (N.D. Cal. 2000).

> The phrase "brick and mortar" is often used to designate a traditional business when contrasting it with a predominantly, or entirely, on-line business. The phrase appears to refer to the historical reliance on conducting commerce within the context of a physical space made from materials such as brick and mortar, as opposed to the modern trend toward conducting commerce in a cyberspace made from computer programs.

Id.

11. *See, e.g.*, Bestbuy.com, *at* http://www.bestbuy.com (providing information regarding the retailer's products and giving customers the option of buying these products on-line).

12. Niva Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 26 U. DAYTON L. REV. 179, 183 (2001) (asserting that "[t]he decentralized nature of the Internet was considered one of its most significant characteristics" and that the Internet was expected to create "a potentially more decentralized flow of information").

factual information on their websites by those they deem unwelcome.[13] However, this data, which website owners are seeking to protect, is material that they have intentionally released for public review.[14] Furthermore, the information itself does not qualify for copyright protection because it does not meet the constitutional requirement of originality.[15] As such, it should be part of the public domain and, therefore, available to anyone without restriction.[16] Any attempt to grant private rights in this information arguably runs afoul of the Intellectual Property Clause and the First Amendment.[17]

Despite this, companies have argued that they have proprietary rights in the information contained on these websites or alternatively on the servers upon which the publicly available websites reside.[18] Furthermore, they have argued that as property owners they alone can decide the terms upon which access is granted to these Internet sites, as well as the way in which the information contained therein can be used.[19] To the extent that any conduct exceeds the scope of these virtually unchecked restrictions, the companies contend that such behavior amounts to hacking—even if it causes no real harm.[20]

In particular, many of these companies have tried to prevent electronic data gatherers from accessing and utilizing the information on their websites.[21] These computerized agents—often referred to as "robots," "spiders," or "crawlers"—can quickly and efficiently collect the public information contained on a website.[22] However, because

---

13. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000) (describing the plaintiff's desire to enjoin the defendant from accessing the plaintiff's database).

14. *See, e.g., id.* (noting that the plaintiff pursued the suit even though it "acknowledge[d] its obligation to provide public access to its customers' contact information").

15. *See infra* Part II (discussing requirements for copyright protection).

16. *See infra* Part VII (proposing an amendment to the Computer Fraud and Abuse Act that would deny protection for factual information on publicly accessible websites).

17. *See infra* Part II (reviewing the constitutional restraints on copyright protection).

18. *See infra* Part V; *see also* Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 574-80 (2001) (discussing cases in which companies sued aggregators of product and pricing information).

19. In one case, for example, the website owner objected to the defendant copying facts from the plaintiff's website and publishing those facts in its own format. *See* Ticketmaster Corp. v. Tickets.com, Inc., No. 99CV7654, 2000 WL 1887522, at *3 (C.D. Cal. Aug. 10, 2000).

20. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (noting that eBay argued that the defendant "interferred with eBay's possessory interest in its computer system" by using data obtained from eBay's website).

21. *See, e.g., id.*

22. *See* O'Rourke, *supra* note 18, at 570 (stating that those tools "allow the engines to amass information more quickly than a manual approach that would require entering each link into the browser and following its path").

software robots are generally used by competitors, as opposed to potential customers, they are often viewed as unwelcome guests.

Nevertheless, choosing to place a publicly accessible website on the Internet should indicate consent to at least a certain amount of access and use of such information by both private and commercial users.[23] Furthermore, the fact that someone or something has a commercial purpose should not determine whether access is proper. This is particularly true in light of the public benefit that accrues from competition in the marketplace.[24] Additionally, these robots are collecting non-copyrightable information that is generally designed to be free.[25]

In this battle for control, companies have recently turned to a new weapon—the Computer Fraud and Abuse Act (CFAA).[26] The CFAA was originally enacted in 1984 as a criminal statute to address hacking and the growing problem of computer crime.[27] In a single, comprehensive statute, it sought to define illegal conduct and provide for criminal liability. The statute has been amended several times, most recently in 2001.[28] One of the most notable changes occurred in 1994 when a civil remedy was added.[29] Congress originally conceived the CFAA as a way to encourage institutions to improve computer security practices and supplement the resources of law enforcement in combating computer crime.[30]

However, the CFAA is now being used to control access to and the use of information contained on publicly available websites.[31] Recent court decisions have allowed website owners to utilize the CFAA to override the carefully balanced provisions of the copyright laws and improperly restrict speech in violation of the First Amendment.[32] Additionally with recent changes to the CFAA, a website owner will often

---

23. *Id.* at 620.

24. *See infra* Part IV; *see also* O'Rourke, *supra* note 18, at 620.

25. Lawrence Lessig, *Foreword to Symposium: Cyberspace and Privacy: A New Legal Paradigm*, 52 STAN. L. REV. 987, 996 (2000).

26. 18 U.S.C. § 1030 (2000 & Supp. 2003).

27. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190 (1984); *see infra* Part III.

28. Pub. L. No. 107-56, § 814, 115 Stat. 366, 382 (2001).

29. Pub. L. No. 103-322, § 290001, 108 Stat. 1796, 2097-99 (1994).

30. 146 CONG. REC. S10,916 (daily ed. Oct. 24, 2001) (statement of Sen. Leahy).

31. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000) (enjoining defendant from accessing publicly available information on plaintiff's website); *see also infra* notes 126-143 and accompanying text (discussing the facts and the holding of *Register.com*).

32. *See Register.com, Inc.*, 126 F. Supp. 2d at 255; *see also infra* notes 317-319 and accompanying text (explaining that a statute protecting factual material may violate the First Amendment).

find that the elements required for a CFAA cause of action are far easier to prove than any other type of potentially applicable claim, including the common law claim of trespass.[33]

This Article argues that, although many of these actions may fall within the literal language of the CFAA, such cases were never intended to be covered by the statute. Additionally, by allowing website owners to protect information that is not protectable under copyright law, the CFAA unconstitutionally overrides the delicate balance of rights between authors and the public. Such a sweeping reading of prohibited acts under the CFAA threatens the free flow of information that belongs in the public domain. As a result, the continued openness of the Internet, along with its attendant benefits, is at risk.

This Article begins in Part II by briefly explaining why the factual information that website owners seek to control is not protectable under copyright law. Next, Part III of this Article examines the history and purpose of the Computer Fraud and Abuse Act. Part IV explores the way in which software robots gather information on the Internet and why companies have tried to limit their use. Part V looks at the elements of a CFAA claim, including the way companies have sought to define unauthorized access under the Act. Part VI discusses the constitutional confines within which Congress can create private property rights in information. Part VI also examines the proprietary rights of publicly accessible website owners and whether such rights should include the right to prohibit software robots from accessing the information contained on their Internet sites or alternatively the servers upon which the websites reside. Part VII suggests language that could be used to amend the CFAA to ensure its constitutionality. Additionally, Part VII reviews and evaluates alternative methods for controlling truly harmful robot behavior.

II. COPYRIGHT LAW

The Copyright Act[34] provides that copyright protection extends to only "original works of authorship," as originality is a constitutional requirement.[35] To be original, the work must be independently created, in other words not copied from another work. Additionally, it

---

33. *See infra* notes 266-296 and accompanying text (discussing changes to the CFAA's definition of loss).

34. 17 U.S.C. § 102 (2000).

35. U.S. CONST. art. I, § 8, cl. 8 (authorizing Congress to "secur[e] for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"); *see also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 346 (1991) (declaring that "[o]riginality is a constitutional requirement").

must possess "at least some minimal degree of creativity."[36] This requirement is not particularly burdensome, as a relatively low level of creativity will usually suffice.[37]

Facts, however, do not even meet this modest threshold. As the Supreme Court made clear in *Feist Publications, Inc. v. Rural Telephone Service Co.*,[38] "[n]o one may claim originality as to facts . . . because facts do not owe their origin to an act of authorship . . . . [T]hey may not be copyrighted and are part of the public domain available to every person."[39] This is because one who reports a particular fact has not created it; he or she has merely discovered its existence.[40] Because data is not "original" in the constitutional sense, it may not be copyrighted.[41] Instead, it remains in the public domain, available to every person.[42]

This is true even if the facts are contained within a work that is copyrightable as a whole. One fundamental principle of copyright law is the "idea-expression" or "fact-expression" dichotomy, which applies to all works of authorship.[43] In the context of factual works, only the author's selection and arrangement may be protected, while the facts themselves may be copied at will.[44] This secures protection for the author's original expression, while allowing others to freely build upon the ideas and information contained within a work without seeking the creator's permission.[45] As the Supreme Court has explained, "[t]his result is neither unfair nor unfortunate, [but] is the means by which copyright advances the progress of science and art."[46] Copyright seeks to reward originality, not effort.[47]

For example, the Copyright Act expressly provides for the protection of compilations.[48] A compilation consists of a collection of preex-

---

36. *Feist*, 499 U.S. at 345 (citing 1 M. NIMMER & D. NIMMER, COPYRIGHT §§ 2.01 [A], [B] (1990)).

37. *Id.*

38. 499 U.S. 340 (1991).

39. *Id.* at 347-48 (citing 1 M. NIMMER & D. NIMMER, COPYRIGHT §§ 2.01 [A], [B] (1990) and Miller v. Universal City Studios, Inc., 650 F.2d 1365, 1369 (5th Cir. 1981)).

40. *Id.* at 347.

41. *Id.*

42. *Id.* at 348 (citing *Miller*, 650 F.2d at 1369).

43. *Id.* at 350.

44. *Id.*

45. *Id.* at 350-51.

46. *Id.* at 350.

47. *Id.* at 359-60 ("[O]riginality, not 'sweat of the brow,' is the touchstone of copyright protection in directories and other fact-based works.").

48. 17 U.S.C. § 103 (2000) (stating that "[t]he subject matter of copyright as specified by section 102 includes compilations and derivative works").

isting data selected and arranged by an author.[49] If the organization of the materials is made independently by the compiler and entails a minimal degree of creativity, such works contain sufficient originality to be entitled to copyright protection.[50] A subsequent compiler, however, is free to use the facts contained in another's work so long as the new work does not include the same selection and arrangement of material.[51] The mere inclusion of a particular fact in a work does not transform that fact into protectable intellectual property.[52]

In the context of a website, even though some elements of an Internet site may be protectable under the copyright law, factual information is supposed to remain in the public domain.[53] For example, a site may contain photographs or illustrations that may be copyrighted. However, information concerning a particular product's price, dimensions, or the sizes in which it is available are merely facts that anyone else should be free to use.[54] Furthermore, the extraction and use of such information is "essential to achieving the constitutional goal of copyright law."[55] The balance of rights in copyright law is rooted in the belief that society is best served by the free flow of information.[56] As facts and ideas constitute the building blocks of knowledge, it is imperative that they remain within the public domain. Despite the recent claims of website owners to the contrary, the use of such information without the website owner's permission should not constitute a criminal act.

III. HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT

In response to a growing wave of hacking incidents and related computer fraud, Congress enacted the first federal computer crime statute in 1984 entitled the Counterfeit Access Device and Computer Fraud and Abuse Act (Counterfeit Access Device Act).[57] Instead of

---

49. *Id.* § 101.

50. *Feist*, 499 U.S. at 348.

51. *Id.* at 349.

52. *Id.* at 350-56.

53. *See id.* at 348 (declaring that "all facts—scientific, historical, biographical—are part of the public domain").

54. *See id.* at 349 ("[T]he very same facts and ideas may be divorced from the context imposed by the author, and restated or reshuffled by second comers, even if the author was the first to discover the facts or to propose the ideas.").

55. J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 129 (1997).

56. *Feist*, 499 U.S. at 349-50.

57. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2000)); Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users"*

identifying and amending every potentially applicable statute affected by advances in computer technology, Congress chose to address the subject in a single statute.[58] "Congress was reluctant to preempt or interfere with local and state computer crime authorities,"[59] therefore, this original legislation was exceptionally narrow in scope.[60]

The statute prohibited unauthorized access to a computer system,[61] but it only applied to "federal interest computers,"[62] generally

---

Have you Ever Heard of It?, 6 RICH. J.L. & TECH. 23, ¶ 13 (2000), *available at* http://www.law.richmond.edu/jolt/v6i5/article2.html.

58. S. REP. NO. 104-357, at 5 (1996).

59. Nemerofsky, *supra* note 57, ¶ 13. All fifty states have some form of computer crime legislation, however the scope of sanctioned conduct ranges from state to state: ALA. CODE §§ 13A-8-100 to -103 (1994); ALASKA STAT. §§ 11.46.200(a)(3), 11.46.484(a)(3), 11.46.740, 11.46.985 (Michie 2002); ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (West 2001); ARK. CODE ANN. §§ 5-41-101 to -108 (Michie 1997); CAL. PENAL CODE §§ 502, 502.01, 1203.047 (West 1999 & Supp. 2003); COLO. REV. STAT. ANN. §§ 18-5.5- 101 to -102 (West 1999 & Supp. 2003); CONN. GEN. STAT. ANN. §§ 53a-250 to –261 (West 2001); DEL. CODE ANN. tit. 11, §§ 931-939 (2001); FLA. STAT. ANN. §§ 815.01-.07 (West 2001 & Supp. 2004); GA. CODE ANN. §§ 16-9-90 to -94 (2003); HAW. REV. STAT. ANN. §§ 708-890 to –895.7 (Michie 1999 & Supp. 2002); IDAHO CODE §§ 18-2201 to -2202 (Michie 1997 & Supp. 2003); 720 ILL. COMP. STAT. ANN. 5/16D-1 to -7 (West 2003); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (Michie 1998 & Supp. 2001); IOWA CODE ANN. §§ 702.1A, 702.14, 714.1, 716.6B (West 2003); KAN. STAT. ANN. § 21-3755 (1995 & Supp. 2002); KY. REV. STAT. ANN. §§ 434.840-.860 (Banks-Baldwin 2003); LA. REV. STAT. ANN. §§ 14:73.1-.5 (West 1997 & Supp. 2003); ME. REV. STAT. ANN. tit. 17-A, §§ 431-433 (West 1983 & Supp. 2002); MD. CODE ANN., CRIM. LAW § 7-302 (2002); MD. ANN. CODE art. 27, § 146 (2002); MASS. GEN. LAWS ANN. ch. 266, §§ 30, 33A, 120F (West 2000); MICH. COMP. LAWS ANN. §§ 752.791-.797 (West 1991 & Supp. 2001); MINN. STAT. ANN. §§ 609.87-.891 (West 2003); MISS. CODE ANN. §§ 97-45-1 to -13 (1994 & Supp. 2003); MO. ANN. STAT. §§ 569.095-.099 (West 1999 & Supp. 2003); MONT. CODE ANN. §§ 45-6-310 to -311 (2003); NEB. REV. STAT. §§ 28-1343 to -1348 (1995); NEV. REV. STAT. ANN. §§ 205.473-.513 (Michie 2001); N.H. REV. STAT. ANN. §§ 638:16 to :34 (1996 & Supp. 2002); N.J. STAT. ANN. §§ 2A:38A-1 to -6 (West 2000), 2C:20-23 to -34 (West 1995); N.M. STAT. ANN. §§ 30-45-1 to -7 (Michie 1997 & Supp. 2003); N.Y. PENAL LAW §§ 156.00-.50 (McKinney 1999); N.C. GEN. STAT. §§ 14-453 to –458 (2002); N.D. CENT. CODE §§ 12.1-06.1-01, 12.1-06.1-08 (1997 & Supp. 2003); OHIO REV. CODE ANN. § 2913.04(B) (Anderson 2002); OKLA. STAT. ANN. tit. 21, §§ 1951-1958 (West 2002); OR. REV. STAT. §§ 164.125, 164.377 (2001); 18 PA. CONS. STAT. ANN. §§ 7603, 7611 (West 2004); R.I. GEN. LAWS §§ 11-52-1 to -8 (2002); S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 2001); S.D. CODIFIED LAWS §§ 43-43B-1 to -8 (Michie 1997 & Supp. 2003); TENN. CODE ANN. §§ 39-14-601 to -603 (1997 & Supp. 2002); TEX. PENAL CODE ANN. §§ 33.01-.04 (Vernon 2003); UTAH CODE ANN. §§ 76-6-701 to -705 (1995); VT. STAT. ANN. tit. 13, §§ 4101-4107 (1998 & Supp. 2003); VA. CODE ANN. §§ 18.2-152.2 to .14 (Michie 1996); WASH. REV. CODE ANN. §§ 9A.52.110-.130 (West 2000); W. VA. CODE ANN. §§ 61-3C-1 to -21 (Michie 2000 & Supp. 2003); WIS. STAT. ANN. § 943.70 (West 1996 & Supp. 2002); WYO. STAT. ANN. §§ 6-3-501 to -505 (Michie 2003).

60. Nemerofsky, *supra* note 57, ¶ 13.

61. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837, 2190-94 (1984) (codified as amended at 18 U.S.C. § 1030 (2000)). The Act made it a felony to knowingly access a computer without authorization or to exceed authorized access in order to obtain classified United States defense or for-

those computers operated by the federal government or a financial institution.[63] This was due to Congress's belief that these computer systems merited special protection, as they contained the most sensitive types of information—namely classified information, financial records, and credit histories.[64]

However, because the Counterfeit Access Device Act only applied to select types of confidential information, it immediately fell subject to harsh criticism from legislators, industry leaders, and law enforcement officials.[65] Additionally, the law was deemed too vague and difficult to use.[66] In fact, only one person was ever indicted under the 1984 Counterfeit Access Device Act.[67]

In response, Congress amended the Counterfeit Access Device Act in 1986 by enacting the Computer Fraud and Abuse Act (CFAA or the Act).[68] The CFAA eliminated some of the Counterfeit Access Device Act's confusing language, defined additional terms, and expanded its scope.[69] In particular, three additional types of computer crimes were added: a computer fraud offense patterned after the federal mail and wire fraud statutes; an offense for the alteration, damage, or destruction of information contained in a federal interest

---

eign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation. *Id.* Additionally, the Act made it a misdemeanor to knowingly access a computer without authorization or to exceed authorized access to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency. *Id.* The 1984 Act also made it a misdemeanor to knowingly access a computer without authorization or to exceed authorized access in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer. *Id.*

62. S. REP. No. 104-357, at 4 (1996). A "federal interest computer" was defined as a computer

> exclusively for the use of a financial institution or the United States Government, or in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government.

18 U.S.C. § 1030(e)(2)(A) (2000).

63. S. REP. No. 104-357, at 4.

64. *Id.* at 3-5.

65. Frank P. Andreano, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem*, 27 AM. J. CRIM. L. 81, 85-86 (1999) (noting that "loan records, corporate account information, or information concerning the bank's deposits in other institutions" were not within the scope of the act).

66. *Id.* at 86; Glenn D. Baker, Note, *Trespassers will be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/L.J. 61, 65 (1993).

67. Baker, *supra* note 66, at 65.

68. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213-16 (1986) (codified as amended at 18 U.S.C. § 1030 (2000)).

69. Nemerofsky, *supra* note 57, ¶ 14.

computer; and an offense for the trafficking of unauthorized computer passwords in certain circumstances.[70]

Over time, however, Congress became increasingly concerned about loopholes in the statute that were arguably permitting some hackers to escape punishment.[71] Additionally, both the type of activities in which hackers were engaging and their range of motivations had greatly broadened, making Congress eager to give the federal government more expansive authority to capture them.[72] As a result, in 1994 Congress again amended the CFAA as part of a more comprehensive omnibus crime bill entitled The Violent Crime Control and Law Enforcement Act of 1994.[73]

Although the CFAA previously had dealt with only conduct related to the unauthorized access of a computer system, the 1994 amendments expanded the coverage of the Act to include the transmission of computer worms and viruses.[74] Moreover, the amendment added a civil remedy in addition to the statute's original criminal sanctions.[75] With the dramatic rise in the number of computer crime cases, the government did not have the ability to pursue all computer crime cases.[76] As such, the civil remedy was designed to provide not only aggrieved individuals with the ability to obtain relief for violations of the Act, but also to increase the deterrent value of the statute.[77]

The sponsors of the amendment made clear, however, that they certainly and expressly did not want to "open the floodgates to frivolous litigation."[78] But at the time this civil remedy was added, the CFAA still only applied to "federal interest computers," namely those computers that contained the most sensitive confidential information and were operated by the government or a financial institution.[79] As a result, the pool of potential plaintiffs was quite limited. This, however, changed two years later.

---

70. Computer Fraud and Abuse Act § 2(d).

71. Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 179 (2000).

72. *Id.*

73. Pub. L. No. 103-322, § 290001, 108 Stat. 1796, 2097-99 (1994).

74. S. REP. No. 104-357, at 4 (1996); Nemerofsky, *supra* note 57, ¶ 26.

75. Pub. L. No. 103-322, § 290001(d), 108 Stat. at 2098. The civil remedy provision allowed victims of computer abuse to maintain actions against the violators to obtain compensatory damages, injunctive relief, or other equitable relief. *Id.*

76. 146 CONG. REC. S10,916 (daily ed. Oct. 24, 2000) (statement of Sen. Leahy).

77. *Id.*

78. *Id.* (quoting 136 CONG. REC. S4,614 (1990) (statement of Sen. Leahy)).

79. *Id.*

The 1996 amendments to the CFAA[80] expanded coverage of the Act to include not only "federal interest computers," but all computers used in interstate commerce.[81] This effectively extended the statute's reach to include any computer connected to the Internet.[82] The change was prompted in part by a growing concern over the amount of financial losses suffered by American companies from the breach of computer security systems.[83] With society's increased dependence on computers, it was becoming clear that computer crime was not just a law enforcement issue, but had economic implications as well.[84]

The sponsors of the bill, therefore, felt it was essential to extend the statute's scope to further protect the confidentiality of computer data, as well as the systems upon which the data resided.[85] References can be found throughout the amendment's legislative history that support the premise that the changes were designed to safeguard the privacy of information.[86] Ultimately, the amendment's sponsors

---

80. The 1996 amendments to the Act were originally entitled the National Information Infrastructure Protection Act of 1996 ("NIIPA"). 142 CONG. REC. S10,889 (daily ed. Sept. 18, 1996) (statement of Sen. Leahy). But when the NIIPA was introduced in 1995, it failed to emerge from the Judiciary Committee Proceedings. Nemerofsky, *supra* note 57, ¶ 28. However, in October of 1996, President Clinton signed the NIIPA into law as part of the Economic Espionage Act of 1996. *See* Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3491-93 (1996).

81. The term "federal interest computer" was replaced with "protected computer." *See* 18 U.S.C. § 1030(2)(c) (2000). A "protected computer" was defined as a computer

> exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in interstate or foreign commerce or communication.

Id. § 1030(e)(2)(A)-(B).

82. Calkins, *supra* note 71, at 180.

83. 142 CONG. REC. S10,889 (daily ed. Sept. 18, 1996) (statement of Sen. Leahy). A December 1995 report from the Computer Systems Policy Project, which included the CEOs from thirteen major computer companies, estimated that breaches of computer security resulted in financial losses of $2 to $4 billion dollars. *Id.* The report also predicted that the numbers were likely to rise to $40 to $80 billion dollars worldwide in the year 2000. *Id.*

84. *Id.*

85. S. REP. NO. 104-357, at 3 (1996) ("I. Purpose: [The amendment] would strengthen the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks.").

86. 142 CONG. REC. S10,889 (statement of Sen. Leahy) ("[W]hile our current statute, in section 1030(a)(2) prohibits misuse of a computer to obtain information from a financial institution, it falls short of protecting the privacy and confidentiality of information on computers used in interstate or foreign commerce and communications."); S. REP. NO. 104-357, at 7 (1996) ("The bill would amend 1030(a)(2) to increase protection for the

hoped that the changes would also help ensure the public's faith in the security of computer networks.[87] Noticeably absent from the legislative history, however, is any suggestion that Congress intended to widen dramatically the protection of the CFAA to include all information and all computer systems on the Internet, such as non-copyrightable data contained on publicly accessible websites.[88] Nevertheless, the statutory language itself was not modified to make clear that the provisions of the CFAA only applied to private, confidential information.[89] Instead, the Act as drafted appears to include protection for any type of information, despite the legislative history to the contrary.[90]

Most recently, the CFAA was amended in October of 2001 by the USA Patriot Act.[91] The USA Patriot Act's provisions were primarily designed to combat terrorism and provide law enforcement with additional investigatory tools.[92] However, the USA Patriot Act also included language from an earlier Senate bill entitled The Internet Security Act of 2000.[93] The USA Patriot Act amended the CFAA in order to rectify some of the more technical ambiguities of the CFAA identified in earlier court cases and to clarify the scope of the civil remedy.[94] However, there were no changes that explicitly restricted the scope of the Act to confidential information,[95] and as such, the CFAA still arguably provides a potentially valuable tool for entities hoping to protect publicly accessible factual information.[96]

---

privacy and confidentiality of computer information . . . [t]he premise of this subsection is privacy protection.").

87. S. REP. No. 104-357, at 7.

88. *See id.* ("[W]here the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws.").

89. 18 U.S.C. § 1030(a)(2)(C), (b) (2000) (stating that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished"). The statute does not exclude information that is not protectable under copyright law. *See id.*

90. *See id.* (failing to describe the type of information protected by the Act).

91. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 814, 115 Stat. 272, 382 (2001).

92. *Id.* § 1.

93. *See* S. 2448, 106th Cong., § 101-102 (2001).

94. *See* 146 CONG. REC. S10,913-916 (daily ed. Oct 24, 2000) (statement of Sen. Leahy) (noting the reasons for modifying the CFAA).

95. *See* 18 U.S.C. § 1030 (2000 & Supp. 2003).

96. *See* Carl S. Kaplan, *Tough Times for Data Robots*, N.Y. TIMES, CYBER L.J., Jan. 12, 2001, *at* http://www.nytimes.com (noting that "the easier it becomes to use the law to thwart robots, the easier it becomes for some companies to lock up or selectively protect publicly available information").

IV. SOFTWARE ROBOTS

Businesses are increasingly targeting software robots for exclusion from their publicly available websites.[97] A software robot is a computer program that can perform tasks on the Internet without human supervision.[98] Some of the more typical functions include compiling results for search engines,[99] filtering for inappropriate content, or obtaining information made publicly accessible on the websites of others.[100] Software robots are capable of executing these tasks at speeds far in excess of what a human can accomplish.[101]

Software robots utilize the same web protocols as any individual would to initially access information from an Internet website.[102] These bots simply request the information from the site, and the queried server usually responds with a copy of the document requested.[103] However, unlike individuals, software robots engage in

---

97. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1073 (N.D. Cal. 2000) (enjoining an online auction aggregation company from copying factual information posted on a publicly accessible website).

98. James C. Luh, *No Bots Allowed!*, EWEEK ENTERPRISE NEWS & REVIEWS, Apr. 16, 2001, *available at* http://www.eweek.com.

99. *See* Nettis Envtl. Ltd. v. IWI, Inc., 46 F. Supp. 2d 722, 724 n.2 (N.D. Ohio 1999). The court defined a search engine as follows:

> [A] special kind of website, containing a database of other known websites, associating certain keywords with each website. The user provides the search engine with [a term] or terms of interest to the user, and the search engine responds with a list of websites on its database associated with the terms submitted by the user.

Id.; *see also* Christine D. Galbraith, *Electronic Billboards Along the Information Superhighway: Liability Under the Lanham Act for Using Trademarks to Key Internet Banner Ads*, 41 B.C. L. REV. 847, 851-53 (2000) (discussing how search engines compile their search results). Some of the most well-known search engines include Excite, Google, AltaVista, and Netscape. *Id.* at 851.

100. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).

101. *eBay*, 100 F. Supp. 2d at 1060-61.

102. O'Rourke, *supra* note 18, at 570 (noting that bots use the same web protocol as the typical Internet user).

103. *Id.* This is not to say, however, that a server will always provide the requested information. Software robots are launched from a particular Internet Protocol (IP) address. David Kramer & Jay Monahan, *Panel Discussion To Bot or Not to Bot: The Implications of Spidering*, 22 HASTINGS COMM. & ENT. L.J. 241, 245 (2000). When the computer requests information from another computer, the requesting computer must offer its IP address to the responding computer in order for a response to be sent. *eBay*, 100 F. Supp. 2d at 1061. If repeated requests come from a particular IP address, this can often signal robotic activity. *Id.* A responding computer that seeks to prohibit robots from accessing its site can then choose to ignore or "block" any further requests from that particular IP address. *Id.* However, this does not usually provide a long-term solution for the responding computer, as IP addresses can change on a daily basis and requesting computers can also route their requests through other servers to appear as though these servers are the source of the original request. *Id.* Additionally, blocking technology also carries a risk of denying requests from IP addresses that a responding computer would actually want to serve. *Id.*

what is referred to as "recursive retrieving" or "automated browsing."[104] Once a web page is obtained from a particular website, the software robot reviews the page and then requests all other pages that are referenced therein.[105]

This repetitive searching often imposes a burden on the requested website's server exceeding that generated by an individual reviewing the very same pages of the website.[106] Website owners have argued that this additional burden could lead to decreased response time for "legitimate users," in other words, those users potentially interested in purchasing goods or services, not those merely competing with the company.[107] Furthermore, these website owners argue that consumption of the system's resources by these unwelcome users could eventually result in an overload that may cause the system to malfunction or "crash."[108] If such a severe malfunction were to occur, data might be lost or service interrupted.[109]

However, in all of the cases brought to date, the burden created by these "illegitimate users" was minimal at best.[110] The websites were not affected in any appreciable way. The servers did not crash, and website users did not experience any noticeable delays in accessing the companies' web pages.[111] Furthermore, the software robots did not cause any actual damage to the servers necessitating system repairs.[112]

Thus, it appears that these owners of publicly accessible websites may be less concerned with actual harm to their computer system and more interested in finding a way to protect themselves from increased competition.[113] However, competition is essential to protecting con-

---

104. O'Rourke, *supra* note 18, at 570; Martijn Koster, *A Standard for Robot Exclusion*, The Web Robots Pages, *at* http://www.robotstxt.org/wc/norobots.htm (last visited Feb. 24, 2004).

105. O'Rourke, *supra* note 18, at 570.

106. *Id.*

107. Maureen A. O'Rourke, *Shaping Competition on the Internet: Who Owns Product and Pricing Information?*, 53 VAND. L. REV. 1965, 1980 (2000).

108. *eBay*, 100 F. Supp. 2d at 1061.

109. *Id.*

110. *See, e.g., id.* at 1063 (noting that while the defendant accessed the plaintiff's website 100,000 times a day, that activity comprised at most 1.53% of the total number of requests); *see also* Kaplan, *supra* note 96 (discussing recent decisions in which courts found that plaintiffs were not significantly burdened by the activities of software robots).

111. Kaplan, *supra* note 96.

112. *Id.*

113. *See* Brief of Amici Curiae in Support of Bidder's Edge, Inc., Appellant, Supporting Reversal, at 6, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (No. 00-15995) [hereinafter Brief of Amici Curiae Professors of Law] ("[E]stablished online merchants have a substantial incentive . . . to interfere with the flow of price and product

sumers.[114] The public benefits from a marketplace that provides a variety of options. In fact, the U.S. government has recognized that maintaining the open architecture of the Internet is essential to fostering valuable competition:[115] "Official decision makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining feature of the new digital marketplace."[116]

This is not to say that a website owner will never be able to show sufficient harm to outweigh the public benefit fostered by open access to information. Where a software robot actually causes a website to malfunction to such a degree that it is unable to serve its customers, a remedy may be appropriate.[117] However, such exceptional claims should not be grounded in the Computer Fraud and Abuse Act, despite the fact that they may fit within the literal language of the CFAA.

V. ELEMENTS OF A CFAA CLAIM

In order to bring a civil action under the Computer Fraud and Abuse Act, a party must be able to prove two main elements. First, a party must show that a defendant has engaged in prohibited conduct.[118] Second, a party must prove that it has suffered sufficient harm as defined by the Act.[119] Before discussing why recent decisions granting publicly available website owners proprietary rights in the access to and use of factual information are not only inappropriate, but arguably unconstitutional, it is worth reviewing the basic requirements of a CFAA claim in more detail.

A. Principal Statutory Provisions upon which Website Owners Base their Claims

Owners of publicly available websites, who have attempted to prevent their competitors from accessing and utilizing the non-copyright-

---

information on the Internet."); O'Rourke, *supra* note 107, at 1981 (noting that "[s]uch claims may have merit or may be asserted as a pretext to mask an anti-competitive intent") (footnote omitted).

114. Brief of Amici Curiae Professors of Law at 3-4, *eBay* (No. 00-15995).

115. *Id.* at 4.

116. William J. Clinton & Albert Gore, Jr., *Framework for Global Electronic Commerce* 2 (July 1, 1997), *available at* http://dcc.syr.edu/ford/course/e-commerce-framework.pdf.

117. Brief of Amici Curiae Professors of Law at 13, *eBay* (No. 00-15995). "Trespass to chattels 'lies where an intentional interference with the possession of personal property has proximately caused injury.'" *Id.* (quoting Thrifty-Tel, Inc. v. Bezenek, 54 Cal. App. 2d 468, 475 (1996)).

118. *See* 18 U.S.C. § 1030 (2000).

119. *Id.* § 1030(g) (2000 & Supp. 2003).

able information contained therein, have based their claims on a number of sections under the CFAA. Although the sections vary slightly, each section requires the plaintiff to prove that the defendant accessed a computer without authorization or exceeded authorized access, which often becomes the primary focus in most CFAA cases.[120] Nonetheless, section (a)(2)(C) appears to be the section that is most applicable in cases involving website owners trying to prohibit a competitor from accessing and utilizing information posted on their Internet site.[121] Additionally, it is probably one of the easiest sections under which to state a claim.

The section prohibits a party from obtaining information by intentionally accessing a computer without authorization or exceeding authorized access.[122] The CFAA does not provide a definition for "information." Despite the fact that the CFAA's legislative history suggests that the statute is designed to protect confidential information,[123] as opposed to all other types of information, the statutory language is not so limited.[124] Furthermore, courts, in their interpretations of this provision, have not made such a distinction, but

---

120. In an attempt to clarify the elements required to bring a civil action under the CFAA, the statute was amended in 2001 to provide that such an action could only be brought "if the conduct involves [one] of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a) (5) (B) (i)." *Id.* At first glance this might appear to restrict civil actions to suits alleging violations of Section (5). However, a more careful reading of the statute reveals that this reference only seeks to incorporate expressly the requirement of "loss" (except in those cases that involve (1) "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment or care of 1 or more individuals"; (2) "physical injury to any person"; (3) "a threat to public health or safety"; or (4) "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security."). *Id.* § 1030(a)(5)(B). Furthermore, the Act provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." *Id.* § 1030(g).

Additionally, there is nothing in the legislative history of the amendment to suggest that the drafters intended to limit civil actions to only those based on conduct prohibited by Section (5). Instead, the legislative history indicates that the change to Section (g) was made only to clarify the type of loss or harm required to maintain a civil action. 146 CONG. REC. S10,916 (daily ed. Oct. 24, 2000).

121. *See* 18 U.S.C. § 1030(a)(2)(C) (2000) (prohibiting unauthorized users from acquiring information from protected computers in other states or countries).

122. *Id.* § 1030(a)(2).

123. *See infra* Part III (discussing references throughout the CFAA's legislative history implying that the statute is designed to protect confidential information).

124. *See* 18 U.S.C. § 1030(a)(2)(c). The statute fails to state that the information must be confidential or privileged to be protected. *Id.*

instead have enjoined defendants from accessing non-copyrightable information freely available from plaintiffs' public websites.[125]

For example in *Register.com, Inc. v. Verio, Inc.*, the plaintiff, Register.com, Inc. (Register.com), sought a preliminary injunction preventing the defendant, Verio, Inc. (Verio), from accessing and utilizing the information contained on its website.[126] Register.com is a domain name registrar, providing customers the ability to register a name in the .com, .net., and .org top-level domains.[127] As part of its obligation as an accredited domain name registrar, Register.com is required under its contract with the national accrediting agency to provide an online, interactive database containing the names, addresses, and phone numbers of all customers who register domain names through its services.[128]

In addition to its domain name registration services, Register.com offers a variety of other related services such as website creation tools, website hosting, and electronic mail.[129] The defendant, Verio, is one of the largest operators of websites for businesses and a leading provider of Internet services.[130] Although Verio is not a domain name registrar, Register.com does compete directly with Verio to provide a variety of other Internet services, including website hosting and development.[131]

In order to target more effectively their marketing and sales efforts, Verio wanted to find a way to recognize those entities in need of web hosting services.[132] Companies that had recently registered a do-

---

125. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000).

126. *Id.* at 241.

127. *Id.*

> A domain name has two parts—a second-level domain and a top-level domain. The second-level domain consists of a term or series of terms, often a descriptive term, a company's name or a brand-name. Top-level domains indicate the type of organization that holds the address and include ".com" for commercial enterprises, ".edu" for educational enterprises, ".org" for non-profit and miscellaneous organizations, ".gov" for government sites, ".net" for networking providers, and ".mil" for military information sites.

Galbraith, *supra* note 99, at 851 (footnote omitted).

128. *Register.com, Inc.*, 126 F. Supp. 2d at 241-42. In order to become an accredited domain name registrar, Register.com, like all registrars, was required to enter into a Registrar Accreditation Agreement (the Accreditation Agreement) with the Internet Corporation for Assigned Names and Numbers (ICANN). *Id.* ICANN is a private, not-for-profit corporation that the U.S. Department of Commerce created to privatize the domain name system. *Id.* at 242 n.1. The Accreditation Agreement sets out all of the responsibilities of a registrar and includes the customer database requirement. *Id.* at 242.

129. *Id.* at 241.

130. *Id.*

131. *Id.*

132. *Id.* at 243.

main name would most likely fall into this category.[133] Therefore, Verio developed a software robot to access the contact information databases each accredited registrar made publicly available on its website, including Register.com's Internet site.[134] The robot collected this information on a daily basis, allowing Verio to identify quickly potential customers for its services.[135]

Register.com objected to Verio's compilation and use of the contact information appearing on its website.[136] In an attempt to prevent the practice from continuing, Register.com sent Verio a letter requesting that it cease and desist its conduct.[137] When Verio refused, Register.com filed suit alleging that Verio's actions violated section (a)(2)(C) of the Computer Fraud and Abuse Act and moved for a preliminary injunction.[138] Register.com alleged that Verio's conduct had resulted in irreparable harm, including lost opportunities to sell additional, competing services to its domain name registrants.[139]

In granting the plaintiff's motion, the court did not analyze the nature of the information at issue. The court did not mention that the information on Register.com's website consisted merely of factual data, such as names and addresses,[140] which is not protectable under copyright law.[141] Additionally, the court did not acknowledge that the data that Verio obtained had been posted by Register.com onto its publicly accessible Internet website.[142] Instead, the court summarily held that Verio's software robots had acquired information from Register.com's website, thus satisfying the specialized requirements of section (a)(2)(C) of the CFAA.[143]

---

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.* at 244.

137. *Id.*

138. *Id.* Register.com also alleged that Verio's actions were prohibited by section (a)(5)(C) of the CFAA. *Id.* at 251. Additionally, Register.com claimed that Verio's conduct violated Section 43(a) of the Lanham Act, and asserted claims for trespass to chattels and breach of contract under the New York common law. *Id.* at 241.

139. *Id.* at 248.

140. *Id.* at 242 (noting that the information in the database consisted of customer names and contact information).

141. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361 (1990) (noting that facts cannot be copyrighted because they are not original creations).

142. *Register.com, Inc.*, 126 F. Supp. at 242 (acknowledging that the information at issue was "freely accessible to the public" on Register.com's website).

143. *Id.* at 252. The court also found that the plaintiff alleged sufficient damage as required by the CFAA and showed that the defendant's conduct was unauthorized as defined by the statute. *Id.*

B. Defining Unauthorized Access

A civil action plaintiff who alleges a violation of the CFAA will be required to prove that the defendant's access to its Internet site was either "without authorization" or "exceed[ed] authorized access."[144] This will generally be the case regardless of whether a plaintiff bases its claim under section (a)(2)(C) or some other section of the Act. The statute does not define "without authorization" and merely defines "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[145] Even more problematic, however, is the fact that the CFAA does not provide any limits on the types of activities that a party may deem to be "unauthorized" nor does it restrict the manner in which these prohibitions are communicated.[146]

As a result, courts have granted website owners broad powers to exclude others from accessing and utilizing the information contained on their publicly accessible websites.[147] These website owners have been given virtually unchecked discretion to define which acts constitute "unauthorized" conduct.[148] Through contracts, the robot exclusion protocol,[149] and direct communication, website owners have been remarkably successful in preventing visitors to their Internet sites from engaging in any conduct they deem undesirable.[150]

1. Mass-Market and Online "Contracts."—Many publicly available websites contain "terms and conditions of use" to which all visitors that access the site are purportedly bound.[151] However, website visitors are typically not required to indicate consent to these provi-

---

144. 18 U.S.C. § 1030(a)(1) (2000).

145. *Id.* § 1030(e)(6).

146. *See generally id.* § 1030(e).

147. *E.g., Register.com, Inc.*, 126 F. Supp. 2d at 242-43, 253 (finding unauthorized access under the CFAA where the defendant violated the terms of the plaintiff's self-created terms of use agreement). The court acknowledged "a movement away from nascent public regulation of the Internet and toward a consensus-based private ordering regime." *Id.* at 247.

148. *Cf.* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 899 (N.D. Iowa 2001) (choosing not to address the statutory meaning of authorization and finding unauthorized access where the plaintiff's self-established "Terms of Service" were violated).

149. *See infra* Part V (defining the "robot exclusion protocol" and how it recently has been utilized).

150. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1073 (2000) (finding unauthorized access where the defendant accessed facts in violation of the plaintiff's stated terms of use and Robot Exclusion Standard).

151. Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 BERKELEY TECH. L.J. 475, 475 (2002).

sions.[152] When such "approval" is necessary, it usually consists of a party clicking on a box marked "I Agree," oftentimes without even being presented with the numerous restrictions to which the user has apparently agreed.[153]

These provisions may prohibit a party from utilizing a software robot to gather data made publicly available by the owner of the website,[154] or they may restrict a visitor from copying uncopyrightable information for any sort of commercial purpose, despite the fact that the copyright laws would clearly allow the party to engage in such conduct.[155] However, courts have not hesitated to enforce contracts of this nature.[156]

For example, in *Register.com, Inc. v. Verio, Inc.*, the plaintiff website owner imposed conditions on the access to and end use of its domain name registrant contact information database.[157] As discussed above, as part of its obligation as an accredited domain name registrar, Register.com was required to provide to the public an online, interactive database containing the names, addresses, and phone numbers of all customers who register domain names through its services.[158] Because the data contained therein consisted solely of facts, the information was not protectable under copyright law.[159] Normally, this would allow a party to freely copy, utilize, and distribute this data.[160]

However, Register.com published terms and conditions governing the use of its domain name registrant database on the home page of its Internet website.[161] These provisions prohibited a party from using the contact information to engage in any commercial advertising or solicitations via direct mail, electronic mail, or by telephone.[162] Additionally, the terms provided that the user, by

---

152. *Id.*

153. *Id.*

154. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 242 (S.D.N.Y. 2000) (discussing Register.com's terms and conditions for users, which prohibit the use of "high volume, automated, electronic processes that apply to Register.com").

155. *See supra* notes 38-42 and accompanying text (explaining that copyright law does not protect facts because they do not meet the originality requirement).

156. *See, e.g., Register.com, Inc.*, 126 F. Supp. 2d at 245-48 (granting Register.com an injunction based on its breach of contract claim).

157. *Id.* at 242-44.

158. *Id.* at 241-42.

159. *See supra* notes 38-56 (discussing the scope of copyright law).

160. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1990) (noting that facts are uncopyrightable public information).

161. *Register.com, Inc.*, 126 F. Supp. at 242-43.

162. *Id.* at 242-43. The terms and conditions read as follows:

> By submitting a . . . query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to: (1) allow,

submitting a request for information from the database, agreed to be bound by the terms and conditions of use.[163]

Verio conceded that its use of the contact information for marketing purposes conflicted with Register.com's posted restrictions.[164] However, Verio claimed that the terms and conditions were unenforceable, as it had never manifested assent to them.[165] Additionally, Verio argued that even under Register.com's policies, it was entitled to access the contact information database.[166] As such, Verio argued that its conduct could not be deemed "unauthorized" and, consequently, it could not be in violation of the CFAA.[167]

The court disagreed, finding that Verio was in fact bound by the terms and conditions posted by Register.com on its Internet site.[168] The court began its discussion by acknowledging that "Register.com's terms of use are clearly posted on its website."[169] Additionally, the court noted that the concluding paragraph of the terms and conditions stated that "by submitting this query, you agree to abide by these terms."[170] The court held that "in light of this sentence at the end of Register.com's terms of use, there can be no question that by proceeding to submit a [request for information], Verio manifested its assent to be bound."[171] The court found it irrelevant that Verio was not asked to click on an icon indicating that it accepted the terms, as Verio did not argue that it was unaware of them.[172]

The court ruled that because Verio had retrieved contact information for the purpose of solicitation in violation of Register.com's posted policies, Verio had violated the CFAA.[173] The court held that even if Verio's initial access to the contact information database could

---

> enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; or (2) enable high volume, automated, electronic processes that apply to Register.com (or its systems). The compilation, repackaging, dissemination or other use of this data is expressly prohibited without the prior written consent of Register.com. Register.com reserves the right to modify these terms at any time. By submitting this query, you agree to abide by these terms.

Id.

163. *Id.*
164. *Id.* at 245.
165. *Id.* at 246.
166. *Id.* at 252-53.
167. *Id.*
168. *Id.* at 248.
169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.*
173. *Id.* at 252-53.

be classified as "authorized," such access would still be rendered "unauthorized," because Verio knew that the data it obtained would be used for a purpose prohibited by the terms and conditions of Register.com's Internet site.[174] The court did not address the fact that the information at issue was uncopyrightable or that it had been made publicly available by Register.com. Instead, the court found that Register.com was entitled to a preliminary injunction based upon its CFAA claim and ordered Verio to comply with all of Register.com's website policies.[175]

The enforcement of contracts protecting noncopyrightable information, similar to the one at issue in *Register.com* has generated a substantial amount of controversy among academic commentators.[176] Although a detailed discussion is beyond the scope of this Article, in part because contracts are only one of the methods by which website owners have been able to define unauthorized conduct under the CFAA, it is worth noting some of the predominate issues involved in this debate. These generally fall into the categories of assent, copyright preemption, and unconscionability.

---

174. *Id.* at 253.

175. *Id.* at 252-53, 255. The injunction provided, in relevant part, that Verio was prohibited from engaging in the following activities:

> [1] Accessing Register.com's computers and computer networks in any manner, including, but not limited to, by software programs performing multiple, automated, successive queries, provided that nothing in this Order shall prohibit Verio from accessing Register.com's WHOIS database in accordance with the terms and conditions thereof; and
>
> [2] Using any data currently in Verio's possession, custody or control, that using its best efforts, Verio can identify as having been obtained from Register.com's computers and computer networks to enable the transmission of unsolicited commercial electronic mail, telephone calls, or direct mail to the individuals listed in said data . . . .

Id. at 255.

176. Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 395-41 (1999) (discussing copyright law and the scope of the public domain); J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 884-913 (1999) (examining the practice of contracting around federal intellectual property law); Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827, 828-89 (1998) (exploring the relationship between contract and copyright law); Maureen A. O'Rourke, *Copyright Preemption After the ProCD Case: A Market-Based Approach*, 12 BERKELEY TECH. L.J. 53, 77-90 (1997) (discussing the competing interests involved in freedom of contract and preservation of the public domain).

a. Assent.—It is black letter law that in order for a contract to be enforceable, a party must have assented to its terms.[177] However, gone are the days when parties sit down and negotiate each and every term of an agreement. The vast majority of contracts today are standard form agreements. Courts have generally enforced these types of contracts, balancing the ideal of fully informed assent against the realties of the marketplace in which obtaining such assent is prohibitively expensive, particularly with mass-market transactions.[178]

However, commentators have expressed concern that actual assent has become increasingly fictitious with some of the new forms of standardized agreements that have emerged in the marketplace.[179] It is difficult to see how a website visitor that has not provided any positive acceptance to the site's terms and conditions can be deemed to have consented to them through the mere use of the Internet site.[180] But recent court decisions have facilitated the enforcement of such contracts.[181] Additionally, the passage of the Uniform Computer Information Transaction Act (UCITA)[182] by some state legislatures[183] has provided additional validation.[184]

---

177. U.C.C. § 2-204(1) (2003). A contract's existence depends on mutual intent to agree. *Id.*

178. O'Rourke, *supra* note 18, at 623-24.

179. *See id.* at 624-65 (noting that in the electronic context "not all users will read the terms, making any assent less than fully informed").

180. *See id.* at 624 (encouraging the adoption of a rule requiring website operators, in order for their terms of use to be enforceable, to provide the terms before allowing access to the website).

181. *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1150-51 (7th Cir. 1997) (upholding arbitration clause in contract included with mail-order computer, despite the fact that the consumer could not view the agreement until after the item arrived); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1455 (7th Cir. 1996) (holding that software distributed with boilerplate license agreement, often called a "shinkwrap contract," is enforceable despite the fact that consumers cannot even view the contract until after the purchase has been made); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305, 315-16 (Wash. 2000) (holding that an arbitration clause in a "shrink-wrap" licensing agreement was enforceable); Westendorf v. Gateway 2000, Inc., No. 16913, 2000 WL 307369, at *5 (Del. Ch. Mar. 16, 2000) (enforcing an arbitration provision contained within a standard form contract accompanying a computer purchased by mail).

182. The Uniform Computer Information Transactions Act (UCITA) is a model contract law for software licenses and other computer information transactions. *See* Pamela Samuelson & Kurt Opsahl, *How Tensions Between Intellectual Property Policy and UCITA Are Likely to be Resolved, in* ECOMMERCE: STRATEGIES FOR SUCCESS IN THE DIGITAL ECONOMY 741, 746-53 (Practising Law Inst. ed., 1999) (providing an overview of UCITA).

183. *See, e.g.*, MD. CODE ANN., COM. LAW I § 22-106 (2002) (adopting UCITA in Maryland).

184. The provisions of UCITA have been heavily criticized for making it even easier for courts to find that a party has assented to contractual provisions. *See* Samuelson & Opsahl, *supra* note 182, at 752-53 (noting that under UCITA contracts can be formed without a "signature, specific language or any specific conduct," thereby significantly expanding the

b. Preemption.—Even if the assent hurdle is cleared, a website owner seeking enforcement of a contract that provides protection beyond that granted by the Copyright Act may still face a preemption challenge.[185] Preemption may be statutorily or constitutionally based.[186] Section 301 of the Copyright Act provides that "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . are governed exclusively by" federal copyright law.[187] Therefore, a state law cause of action is preempted by the Copyright Act if the rights asserted under it are "equivalent" to those protected by the Copyright Act, and the work involved falls within the "subject matter" protected by the Copyright Act.[188] To the extent a state law contains an "extra element" not found in copyright law, courts generally will hold that the state law is not preempted by the Copyright Act.[189]

Many websites, including the one involved in *Register.com* contain terms and conditions that prohibit the use of all information contained on the site for any sort of commercial purpose, including uncopyrightable facts.[190] However, if the data at issue is not entitled to copyright protection, the Copyright Act allows the information to be freely copied and utilized for even commercial purposes.[191] By attempting to restrict rights granted by the Copyright Act through contract law, website owners are arguably displacing the carefully balanced provisions of the Copyright Act and, in its place, substituting their own privately legislated intellectual property laws.[192] As such, commentators have argued that enforcement under state law may be

---

concept of assent). At the time of this writing, UCITA had been adopted by Maryland and Virginia, and legislation had been introduced in Arizona, Illinois, Maine, New Hampshire, New Jersey, Oregon, Texas, and the District of Columbia.

185. *See, e.g.*, Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998) (holding that the Copyright Act preempts state law where (1) the rights asserted by the plaintiff under state law are equivalent, and (2) the work in question is covered within the subject matter of the Copyright Act).

186. Maureen A. O'Rourke, *Fencing Cyberspace: Drawing Borders in a Virtual World*, 82 MINN. L. REV. 609, 694 (1998).

187. 17 U.S.C. § 301(a) (2000).

188. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1072 (N.D. Cal. 2000) (citing *Kodadek*, 152 F.3d at 1212).

189. *See* Mayer v. Josiah Wedgwood & Sons, Ltd., 601 F. Supp. 1523, 1535 (S.D.N.Y. 1985) (discussing the "extra element" test for preemption).

190. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 242-43 (S.D.N.Y. 2000).

191. *See* 17 U.S.C. § 107 (2000) (delineating the "fair use" policy).

192. O'Rourke, *supra* note 186, at 694-97 (discussing the conflict between the use of contractual use-restriction provisions and the Copyright Act).

preempted to the extent that these contracts give website owners more rights than copyright law provides.[193]

However, courts have not been particularly receptive to this line of reasoning.[194] Instead courts have found that these contracts are not preempted because they contain an "extra element," namely the promises of each of the parties to the agreement.[195] In *ProCD, Inc. v. Zeidenberg*,[196] the leading case on the subject of section 301 copyright preemption, the court distinguished contractual rights and copyright rights by stating that "[c]ontracts . . . generally affect only their parties; strangers may do as they please, so contracts do not create exclusive rights."[197]

But even if a contractual provision survives section 301 preemption, it still may be constitutionally preempted.[198] A contractual term may be constitutionally preempted if its enforcement would "stand as an obstacle to the accomplishment of the full purposes and objectives of Congress" in enacting a particular statute.[199] Website owners frequently include a provision in the terms and conditions that any use of software robots to gather information on the Internet site is prohibited.[200] There is no copyright right to employ software robots, therefore, relinquishing one's ability to use one would not implicate an "equivalent right."[201] However, enforcement of the prohibition would remove a method by which a website visitor could exercise its right to copy uncopyrightable information.[202] The fact that the website owner would alternatively allow the Internet site's content to be manually

---

193. *See id.* at 687 (noting that in the Internet context "[b]oilerplate notices against linking may be . . . preempted by federal copyright law"); Elkin-Koren, *supra* note 12, at 200 ("A license that restricts use of (otherwise unprotected) information could be preempted under copyright law.") (footnote omitted).

194. *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1150 (7th Cir. 1997) (holding that purchasers were bound by a contract not seen until they opened the box containing their purchase); *see also* ProCD, Inc. v. Zeidenburg, 86 F.3d 1447, 1455 (7th Cir. 1996) (holding that contractual provisions were not preempted by the Copyright Act).

195. *See, e.g., ProCD*, 86 F.3d at 1454-55.

196. 86 F.3d 1447 (7th Cir. 1996).

197. *Id.* at 1454 (internal quotation marks omitted).

198. *See* O'Rourke, *supra* note 18, at 626 (discussing the application of constitutional preemption).

199. *Id.* (quoting Hines v. Davidowitz, 312 U.S. 52, 67 (1941)).

200. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1060 (discussing eBay's "User Agreement").

201. O'Rourke, *supra* note 107, at 2000. The Copyright Act protects rights that are "equivalent to any of the exclusive rights within the general scope of copyright." 17 U.S.C. § 301(a) (2000).

202. O'Rourke, *supra* note 107, at 2000.

indexed may not necessarily save the software robot restriction from preemption.[203]

c. Unconscionability.—Another potential argument for the invalidation of restrictions such as those found in *Register.com* is that they are unconscionable. Traditionally, a term is defined as "unconscionable" if it is unduly harsh, commercially unreasonable, or grossly unfair given the existing circumstances.[204] However, some commentators have suggested a more refined "public-interest unconscionability" doctrine in which standard form contracts that contain terms that impede competition or undermine present or future public-interest uses of information should not be enforced.[205] Terms and conditions that prevent software robots from accessing and utilizing non-copyrightable information may satisfy either test of unconscionability.[206] Requiring all website visitors to consent to such a prohibition before being permitted to access or use otherwise unprotectable information arguably rises to the level of being "unduly harsh" or "commercially unreasonable."[207] This is due to the fact that these types of contractual restrictions look less like a means of protecting a website owner's Internet site and more like an attempt to prevent competition.[208] Furthermore, as competition is essential to protecting consumers,[209] enforcement of a contractual provision that hinders it is not in the public's best interest.[210]

2. "Traditional" Contracts.—It is not just mass market licenses that have formed the basis for CFAA claims. In *EF Cultural Travel BV v. Explorica, Inc.*,[211] the First Circuit held that an employee's confiden-

---

203. *Id.* (citing Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160, 167 (1989)). The *Bonito* Court held that a Florida statute prohibiting one method of duplicating boat hulls was preempted by the federal Patent Act. *Bonito*, 489 U.S. at 168.

204. BLACK'S LAW DICTIONARY 1524-25 (6th ed. 1990) (defining unconscionability as a "doctrine under which courts may deny enforcement of unfair or oppressive contracts"); *see also* Campbell Soup Co. v. Wentz, 172 F.2d 80 (3d Cir. 1948) (applying the doctrine of unconscionability to a contract for the sale of chattels).

205. *See, e.g.*, Reichman & Franklin, *supra* note 176, at 929-32 (proposing the doctrine of public-interest unconscionability).

206. *See id.* at 931 (explaining that contract terms that unreasonably deviate from commercially accepted practices are unconscionable).

207. O'Rourke, *supra* note 107, at 2000.

208. *See id.* (stating that "[t]he blanket exclusion of spiders employed by shopbots may hamper competition by restricting the flow of pricing information").

209. *See supra* Part IV (discussing consumer benefits from competition).

210. *See* Elkin-Koren, *supra* note 12, at 182 (asserting that "[a] noncompetitive market of virtual gatekeepers could compromise open access and cause inefficiencies in electronic commerce").

211. 274 F.3d 577 (1st Cir. 2001).

tiality agreement defined the contours of "authorized" conduct for the purposes of a CFAA action.[212] However, as discussed below, the court's decision appears to be erroneous.

The plaintiff, EF Cultural Travel BV (EF), has been in business for more than thirty-five years and is the world's largest private student travel organization.[213] In early 2000, the defendant, Explorica, Inc. (Explorica), was formed and began to compete with EF in the field of global tours for high school students.[214] Several of EF's former employees were hired by Explorica, including Philip Gormley, the former vice president of information strategy at EF, who became the vice president of Explorica.[215]

Gormley believed that the best way to compete with EF would be to charge less for equivalent travel packages.[216] In order to do this, Gormley needed to obtain the prices for each of EF's tours.[217] Gormley considered several ways to obtain EF's prices, but ultimately decided that the most efficient method would be to use a software robot to gather the non-copyrightable information from EF's publicly accessible website.[218] Explorica hired its Internet consultant to design the program and then used the program twice, first to retrieve the 2000 tour prices and then the 2001 prices.[219] EF did not, however, suffer any computer slowdowns or loss of data as a result of Explorica's robotic activity.[220]

Upon learning of Explorica's actions,[221] EF filed suit against Explorica alleging violations of the CFAA and sought a preliminary injunction barring Explorica from using its software robot on EF's website.[222] The district court granted the injunction on the grounds that the manner in which Explorica accessed EF's website was "unauthorized," as it likely violated a confidentiality agreement between

---

212. *Id.* at 583-85.

213. *Id.* at 579.

214. *Id.*

215. *Id.*

216. *Id.*

217. *Id.*

218. *Id.* Gormley also considered the following methods of gathering EF's prices: (1) "[M]anually keying in the information from EF's brochures and other printed materials; [(2)] . . . [U]sing a scanner to record the information; [(3)] . . . [M]anually searching . . . EF's website" for the price of each tour offered by EF. *Id.*

219. *Id.* at 579-80.

220. *Id.* at 584.

221. The court noted that "[t]he development and use of the scraper [Explorica's software robot] came to light about a year and a half later during [unrelated] state-court litigation." *Id.* at 580.

222. *Id.*

Gormley and EF.[223] Explorica appealed the decision to the First Circuit.[224]

In affirming the district court's decision, the appellate court first reviewed the terms of the confidentiality agreement at issue.[225] The agreement provided that Gormley was not to disclose or use any "Confidential or Proprietary Information."[226] This term was defined as "any trade or business secrets or confidential information of EF" or "any technical, business, or financial information, the use or disclosure of which might reasonably be construed to be contrary to the interests of EF."[227] The court held that the record contained two communications from Gormley to Explorica's Internet consultant that "seem[ed] to rely on information about EF to which he was privy only because of his employment there."[228]

First, the court pointed to an e-mail from Gormley to the Internet consultant in which he inquired if a member of the company could write a software robot program and also stated that he would be available to work with whomever would design it.[229] The second communication consisted of another e-mail from Gormley to the Internet consultant providing a link to the webpage on EF's publicly accessible Internet site that contained an interactive database that a website visitor could use to obtain EF's tour prices.[230] The information gathered

---

223. *Id.* at 580-82. Incredibly, the district court also held that EF's use of a copyright symbol on one of the pages of its website, along with a link directing users with questions to contact the company, provided notification that use of a software robot was unauthorized. *Id.* at 580. The district court stated that it furnished a "clear statement [that] should have dispelled any notion a reasonable person may have had that the 'presumption of open access' applied to information on EF's website." *Id.* On appeal, the First Circuit did not review this basis for finding that Explorica had engaged in "unauthorized" conduct in violation of the CFAA. *Id.* at 582.

Additionally, the appellate court did not review the district court's finding that EF utilized "technical restraints" to notify Explorica that software robots were prohibited on EF's Internet site. *Id.* The opinion does not specify the types of "technical restraints" EF used, but this most likely included use of the software robot exclusion protocol. *See infra* Part V (providing a discussion of the use of this mechanism).

224. *EF Cultural Travel BV*, 274 F.3d at 578.

225. *Id.* at 582.

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.* The e-mail stated: "[m]ight one of the team be able to write a program to automatically extract prices . . . ? I could work with him/her on the specification." *Id.*

230. *Id.* Gormley's e-mail provided as follows:

> Here is a link to the page where you can grab EF's prices. There are two important drop down menus on the right . . . . With the lowest one you select one of about 150 tours. * * * You then select your origin gateway from a list of about 100 domestic gateways (middle drop down menu). When you select your origin gateway a page with a couple of tables comes up. One table has 1999-2000 prices and

from this page included various tour codes, which EF claimed were confidential.[231]

The court held that these e-mails provided "ample evidence that Gormley provided Explorica proprietary information about the structure of the website and the tour codes" despite the court's acknowledgement that "gathering manually the various codes through repeated searching and deciphering of the URLs[232] theoretically may be possible."[233] According to the court, further evidence that the tour codes were confidential was illustrated by the fact that "[a]n uninformed reader would regard the tour codes as nothing but gibberish."[234] Moreover, the court noted that "[a]lthough the codes can be correlated to the actual tours and destination points, the codes standing alone need to be 'translated' to be meaningful."[235] The court concluded by finding that "Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."[236] As such, the court held that Explorica's actions were "unauthorized" and that the district court's issuance of an injunction for violation of the CFAA was proper.[237]

The court's reasoning in this case appears to be misguided. Despite the court's conclusion that Gormley transferred proprietary information to its Internet consultant,[238] it seems that Gormley provided nothing more than the Internet address on which the publicly available database was located and instructions for its use.[239] This certainly does not resemble the type of information that only an em-

---

> the other has 2000-2001 prices. * * * On a high speed connection it is possible to move quickly from one price table to the next by hitting backspace and then the down arrow.

Id.

231. *Id.*

232. URL is the acronym for "uniform resource locator," the global address of documents and other resources on the Internet. *Id.* at 583 n.13. For example, the URL for book-seller Barnes and Noble's website home page is "http://barnesandnoble.com," while the URL for the page listing the results of a search for all books on "computer hacking" is: http://search.barnesandnoble.com/booksearch/results.asp?WRD=computer+hacking&userid=**********" (author's actual ten digit user identification number removed from URL and replaced with asterisks).

233. *Id.* at 583.

234. *Id.*

235. *Id.*

236. *Id.*

237. *Id.* at 583-84.

238. *Id.* at 583.

239. *Id.* at 582 (referring to the e-mail from Gormley to Explorica's Internet consultant in which Gormley provided the link to EF's prices).

ployee of EF would be privy to, instead it would appear that any individual who was remotely computer savvy could locate EF's publicly available tour price database on its Internet site and navigate through it to obtain the cost of each tour without much difficulty.[240]

Additionally, the fact that the average website visitor would not make use of the tour codes provided on the website,[241] does not transform this uncopyrightable data into proprietary information. Although Gormley may have been better able to organize and utilize the tour price information gathered from EF's website with knowledge of the tour codes, nothing in the opinion indicates that these codes or the tour prices were not available to members of the general public. It would therefore seem difficult to characterize this information as "confidential" or "proprietary."

It appears that EF's CFAA claim was a thinly veiled attempt to prevent legitimate competition.[242] Explorica's software robots were unwelcome visitors, not because they caused harm to EF's computer system, but because the information they gathered allowed Explorica to compete more effectively against EF in the high school global tours market.[243] It is hard to see how utilizing that which looks like publicly accessible information runs afoul of Gormley's employment agreement.[244] It seems that the only real injury EF may have suffered as a result of Explorica's conduct was harm to its bottom line.

3. Robot Exclusion Protocol.—As discussed above, although a software robot utilizes the same web protocols as an individual in initially accessing information from an Internet site, they gather information from a website in a different manner.[245] As a result, while all "traditional" visitors to a website may be asked to click "I Agree" to an Internet site's terms and conditions, a software robot's presence may not activate such a request from the website.[246] Further complicating matters for a website owner seeking to prohibit software robots from accessing and utilizing information from its Internet site, a software

240. *See id.* at 579 (noting that tour information could be acquired by manually searching EF's website).

241. *Id.* at 583.

242. *See* Elkin-Koren, *supra* note 12, at 181-82 (drawing similar conclusions about eBay's CFAA claim in *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000)).

243. *See id.* (noting that the plaintiff in *eBay* was similarly motivated to "preserve its dominance in the online auction industry").

244. *See EF Cultural Travel BV*, 274 F.2d at 582-83 (describing the information accessed by Gormley and the terms of the confidentiality agreement between Gormley and EF).

245. *See supra* Part IV; *see also* O'Rourke, *supra* note 18, at 570-71 (describing the use of automated software tools to extract data).

246. O'Rourke, *supra* note 18, at 570-71.

robot may never actually view the webpage that contains the Internet site's prohibitions against these electronic agents.[247]

Most software robots will, however, see a specially formulated "robots.txt" file upon accessing a website.[248] This document provides directives indicating which parts of the Internet site the owner does not want the robot visiting and is known as the "Robot Exclusion Protocol."[249] But nothing prevents a software robot from ignoring these instructions and crawling the entire site.[250] In fact, the Robot Exclusion Protocol creators designed it to be a voluntary standard.[251]

Regardless, it appears courts may be inclined to give the protocol legal effect.[252] In *eBay, Inc. v. Bidder's Edge, Inc.*, the court held that eBay "explicitly notifies automated visitors that their access is not permitted."[253] The court noted that eBay utilized the Robot Exclusion Protocol to inform software robots that access to its website was unauthorized.[254] Although the court's decision was in the context of a trespassing claim, it would seem that this same analysis would be applicable to eBay's CFAA claim as well.[255]

Once again, however, enforcement of the Robot Exclusion Protocol gives the website owner the power to exclude anyone from its Internet site that it deems undesirable.[256] There is no requirement that the protocol be drafted in such a way to limit its application to robotic activity that could cause actual damage to a computer system.[257] Instead, it can be used to prevent software robots from accessing and

---

247. *Id.* at 572-73.

248. Koster, *supra* note 104. Koster helped develop the Robot Exclusion Protocol and maintains it to this day. Luh, *supra* note 98.

249. Koster, *supra* note 104.

250. *Id.*; Luh, *supra* note 98.

251. Koster, *supra* note 104.

252. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000); *see also* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 580-81 (1st Cir. 2001) (discussing the district court's decision to issue a preliminary injunction on a CFAA claim based in part on its finding that the defendant had "bypassed technical restrictions embedded in the website"—most likely referring to the Robot Exclusion Protocol).

253. *eBay*, 100 F. Supp. 2d at 1070.

254. *Id.* at 1061.

255. *Id.*; *see also* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 28-32 (2000) (discussing courts' use of the trespass cause of action in disputes over computer and Internet access).

256. Luh, *supra* note 98 (stating that the "Robot Exclusion [Protocol] . . . lets Web site owners tell robots where to go and where not to go on their sites").

257. *See id.* (noting that the Robot Exclusion Standard is not really a "standard," as it is not mandatory).

utilizing factual information on an Internet site that is not otherwise protectable, to the detriment of the general public.[258]

4. Direct Communication.—A website owner seeking to control access to and the use of information on its Internet site is not limited to contracts or use of the Robot Exclusion Protocol to notify software robots that they are unwelcome.[259] Courts have held that website owners can use a number of more direct methods to notify a specific party that their electronic data gathering is not permitted.[260] For example, in *eBay*, the court found that eBay had contacted defendant Bidder's Edge by telephone and letter demanding that it cease any further robotic activity.[261] The court held that it was therefore irrelevant that Bidder's Edge may not have assented to the terms and conditions of eBay's website that prohibited the use of software robots, as Bidder's Edge had been "repeatedly and explicitly notified [that] its use of eBay's computer system was unauthorized."[262]

Additionally, in *Register.com, Inc. v. Verio, Inc.*, the court ruled that Register.com's Internet site's terms of use may not have specifically forbidden the use of search robots.[263] However, the court still held that Verio had been notified that such use was prohibited.[264] The court found that it was "clear since at least the date this lawsuit was filed that Register.com d[id] not consent to Verio's use of a search robot," and that Verio was "on notice that its search robot [was] unwelcome."[265] The court ruled that "Verio's future use of a search robot to access the database exceed[ed] the scope of Register.com's consent" and would be unauthorized.[266] As such, the court issued an injunction on Register.com's CFAA claim, prohibiting Verio from ac-

---

258. *See id.* (citing an industry expert who argues that use of the Robot Exclusion standard as a "no trespassing sign" could chill the free flow of information on the Internet).

259. *See, e.g., eBay, Inc.*, 100 F. Supp. 2d at 1062 (referring to eBay's contacting of Bidder's Edge by phone and by letter to notify it that robot use was prohibited on eBay's website).

260. *See id.*

261. *Id.* at 1062.

262. *Id.* at 1068, 1070.

263. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 249 (S.D.N.Y. 2000). Register.com's terms and conditions required a party utilizing its contact information database to agree that it would not "use this data to . . . enable high volume, automated, electronic processes that apply to Register.com (or its systems)." The court also found that "[a]lthough Verio uses an automated process to collect the . . . data it does not then use the collected data to enable an automated process[.]" *Id.* (emphasis omitted). Instead, "[o]nce Verio's software robot secures the . . . information from Register.com's systems, it has completed its automated process with respect to Register.com's systems." *Id.*

264. *Id.*

265. *Id.*

266. *Id.* at 249, 251.

cessing its publicly accessible online database by means of a software robot.[267]

C. *"Loss"*

A civil action plaintiff stating a CFAA claim must not only be able to prove that a defendant has engaged in prohibited conduct, but must also prove that it has suffered sufficient harm.[268] Under the CFAA, a plaintiff must be able to show that the defendant's conduct has resulted in a loss of $5000 by the plaintiff.[269] Prior to the 2001 USA Patriot Act amendments, however, there was some uncertainty as to when the statutory minimum was applicable and how it should be calculated.[270] This was due in large part to a combination of organizational problems and statutory ambiguities inherent in prior versions of the CFAA.[271]

Earlier versions of the Act provided that in order to bring a civil action, a plaintiff must have suffered "damage or loss."[272] The CFAA defined "damage" as "any impairment to the integrity or availability of data, a program, a system, or information" that causes loss aggregating at least $5000 in value during any one-year period to one or more individuals.[273] However, the term "loss" was not defined.

---

267. *Id.* at 252.

268. *See* 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. 2003) (requiring CFAA plaintiff to demonstrate loss of at least $5000).

269. 18 U.S.C. § 1030(g) (Supp. 2003). Section (g) provides in part: "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a) (5) (B)." *Id.* Section (a) (5) (B) (i) provides: "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." *Id.* § 1030(a)(5)(B)(i).

270. *See infra* notes 274-288 (discussing cases in which courts construed the meaning of "loss" under the CFAA).

271. *See, e.g.*, Andreano, *supra* note 65, at 86 (discussing problems associated with the 1984 CFAA).

272. 18 U.S.C. § 1030(g) (1994 & Supp. 1996) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

273. 18 U.S.C. § 1030(e)(8)(A) (1994). The term damage was also defined as "any impairment to the integrity or availability of data, a program, a system, or information, that—

. . .

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety."

Id. § 1030(e)(8)(b)-(d).

However, in the context of website owners attempting to prevent their competitors from accessing and utilizing information contained on their Internet sites, only Section

As a result, a number of cases arose regarding the issue of whether the $5000 statutory minimum applied to "loss" or only "damage."[274] Civil action plaintiffs argued that, although the $5000 threshold may be applicable to cases involving "damage," a party who has suffered "loss" should not be required to prove that it met the statutory minimum.[275] Most courts, however, were not receptive to this line of reasoning, and held that the $5000 statutory minimum applied to civil actions regardless of whether the harm was pled as "loss" or "damage."[276]

Prior to the 2001 amendments, courts also struggled with determining the types of harm that could be included in calculating the $5000 statutory minimum. For example, could the costs of investigating any possible harm caused by a defendant's conduct be included? Additionally, what about computer time lost by a plaintiff as a result of repairs needed because of a defendant's actions? Or were only the costs specified in the definition of "damage" allowed, namely, expenditures directly related to any impairment to the actual computer system or the availability of data?

Courts faced with this issue differed widely over the types of harm that could be included in determining whether the monetary threshold had been met.[277] Others avoided this statutory ambiguity by ar-

---

(A) ("causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals") is applicable. *See id.* § 1030(e)(8)(A).

274. *See infra* notes 275-276 and accompanying text (outlining cases demonstrating this conflict).

275. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 520 (S.D.N.Y. 2001) (noting the plaintiff's argument that "loss" is distinct from "damage" under § 1030(g)).

276. *See id.* at 522 (holding that any loss actionable under the CFAA is subject to the Act's damage minimum); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) (finding that the statute is ambiguous on the issue of whether loss is subject to the $5000 statutory minimum, but that the context of the statute requires an inclusion of "loss" within the harm threshold); Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 678 (E.D. Tex. 2001) (holding that the $5000 statutory minimum is applicable regardless of whether harm is pled as "loss" or "damage"); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001) (stating that in order to bring a civil action, a plaintiff must suffer "damage" as defined under the Act and interpreting "loss" to mean irreparable damage).

277. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584-85 (1st Cir. 2001) (holding that diagnostic measures taken by the plaintiff to assess the defendant's access to its website could be included in calculating the $5000 statutory threshold); *In re Intuit*, 138 F. Supp. 2d at 1281 (declaring that the definition of loss is limited to "irreparable damage" and that a more expansive definition would render the term "damage" superfluous); *In re DoubleClick Inc.*, 154 F. Supp. 2d at 521-22 (citing legislative history for support of its decision that "loss" can include more than just the cost of actual repairs to a computer system); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126-27 (W.D. Wash. 2000) (adopting an expansive definition of "loss" to meet the monetary

guably stretching the logical boundaries of the facts and law in order to find that the plaintiff had alleged sufficient "damage" as defined by the Act, namely, harm to computer data or the system itself.[278] For example, as discussed above, in *Register.com, Inc. v. Verio, Inc.*, the plaintiff website owner brought suit against one of its competitors for utilizing a software robot to collect non-copyrightable data contained on its publicly accessible website.[279] The defendant's conduct did not, however, cause the plaintiff's system to shutdown or result in the corruption of any data.[280]

In an attempt to prove that the $5000 threshold had been met, the plaintiff submitted the declaration of its Vice President for Technology, Robert Gardos, who estimated that the defendant's activities had resulted in the diminishment of 2.3% of the plaintiff's system resources.[281] But during discovery, it was determined that the plaintiff's Vice President had not taken measurements of either the capacity of the plaintiff's computer system or the portion of that capacity that was consumed by the defendant's search robots.[282] Instead, the plaintiff's Vice President admitted that the numbers he used were "all rough estimates" in arriving at his conclusion that the defendant's search robots occupied a certain percentage of the plaintiff's system capacity.[283]

Despite the court's acknowledgement that the plaintiff's vice president's estimations had been "thoroughly undercut,"[284] the court still found that the $5000 threshold had been met.[285] The court stated that "[*i*]*f* the strain on [the plaintiff's] resources generated by robotic searches becomes large enough, it *could* cause [the plaintiff's] computer systems to malfunction or crash. Such a crash would satisfy [the CFAA's] threshold requirement that a plaintiff demonstrate $5000 in economic damages."[286] Based on this mere possibility of future harm, the court determined that the plaintiff had satisfied the

---

threshold); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252 n.12 (S.D.N.Y. 2000) (holding that lost goodwill or business could be included in calculation of the statutory minimum absent the impairment or unavailability of data or systems).

278. *See, e.g., Register.com, Inc.*, 126 F. Supp. 2d at 252 (noting that harm based on the potential for future harm can be included in the calculation of damages under § 1030(g)).

279. *Id.* at 243-44.

280. *Id.* at 249-50.

281. *Id.* at 249.

282. *Id.* at 249-50.

283. *Id.*

284. *Id.* at 249.

285. *Id.* at 252.

286. *Id.* (emphasis added).

statutory minimum level of damage necessary for a CFAA claim.[287] The court went on to issue an injunction that prohibited the defendant's software robots from searching the plaintiff's publicly accessible website.[288]

The 2001 amendments to the Computer Fraud and Abuse Act did not remove the $5000 threshold, but instead arguably made it easier to meet.[289] The USA Patriot Act[290] resolved the statutory ambiguity that had perplexed the courts regarding how the statutory minimum should be calculated by defining "loss" and providing that all loss should be included in determining whether the statutory minimum is met.[291] Currently, the CFAA defines loss as "any reasonable

---

287. *Id.*

288. *Id.*

289. The 2001 amendments made clear that all parties bringing a civil action must prove that they suffered a $5000 loss except in those cases that involve (1) "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals"; [2] "physical injury to any person"; [3] "a threat to public health or safety"; or (4) "damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(a)(5)(B)(ii)-(iv) (Supp. 2003). None of these exceptions, however, are generally applicable to a case involving a website owner attempting to prevent parties from accessing and utilizing information contained on its Internet site.

290. Pub. L. No. 107-56, 115 Stat. 272 (2001).

291. *See* Pub. L. No. 107-56, § 814, 115 Stat. at 382; 18 U.S.C. § 1030 (Supp. 2003). It should be noted that the 2001 amendments resolved another statutory ambiguity related to the statutory threshold, namely, whether the $5000 minimum could be satisfied through a related course of conduct, rather than a single act. The issue arose in a series of class action suits with courts differing in how the CFAA should be interpreted. *See* Hayes v. Packard Bell NEC, Inc., 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001) (holding that the CFAA required an allegation that the defect caused $5000 worth of damage to each protected computer, not $5000 in the aggregate); Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 678 (E.D. Tex. 2001) (determining that in order for the statutory minimum to be met, at least one member of the plaintiff class must have suffered $5000 in damage, and if so, any other individual who suffered damage may bring a claim, even if his or her own damage is less than $5000); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001) (holding that the CFAA only allows damages and losses to "be aggregated across victims and over time for a single act"); *In re* Toys R Us, Inc., Privacy Litig., No. C-00-2746, 2001 U.S. Dist. LEXIS 16947, at *34 (N.D. Cal. Oct. 9, 2001) (holding that each plaintiff did not have to suffer damage of $5000 to meet the statutory threshold and that losses caused by the same type of act by the defendant may be aggregated); *In re* Am. Online, Inc., 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001) (ruling that $5000 statutory threshold can be aggregated among the various members of the plaintiff class).

The USA Patriot Act amended the CFAA to provide that the $5000 damage threshold is satisfied through loss resulting from a related course of conduct affecting one or more protected computers for purposes of an investigation, prosecution, or other proceeding brought by the United States only. 18 U.S.C. § 1030(a)(5)(B)(i) (Supp. 2003). The implication therefore appears to be that a single act, not a related course of conduct, must be alleged by an individual bringing a civil action, as opposed to the government, in order to meet the statutory loss requirement.

cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[292] The legislative history evinces Congress's intent behind the expansive definition was to ensure that a court considers all of a hacking victim's losses when determining whether the $5000 minimum is satisfied.[293]

As a result, the owner of a publicly available website that wants to completely bar its competitors from accessing and utilizing the information contained therein, no longer has to sit by and hope that its claim will be heard by a judge willing to engage in the same analysis that the *Register.com* court employed. Instead, website owners themselves can ensure that they have fulfilled the $5000 statutory threshold. All a website owner need do is to hire a firm to conduct a "damage assessment" following detection of robotic activity.[294] As the statute expressly provides that all charges related to such an assessment are to be included in computing the minimum harm required to bring a civil suit,[295] the website owner will easily satisfy the first element of a civil claim under the CFAA regardless of whether the software robot caused any appreciable harm to its computer system.[296] The requirement of harm under the CFAA has therefore become virtually non-existent. For this very reason, a CFAA claim becomes more attractive to website owners than most other types of claims brought against their competitors, including trespass to chattels.[297]

---

292. 18 U.S.C. § 1030(e)(11) (Supp. 2003).

293. 146 CONG. REC. S10,913, S10,916 (daily ed. Oct. 24, 2001) (statement of Sen. Leahy).

294. *See* 18 U.S.C. § 1030(e)(11) (Supp. 2003) (including among the items that constitute a "loss" reasonable costs in conducting damage assessments). This assumes of course that the damage assessment costs at least $5000. It would appear, however, that this would more than likely be the case.

295. *Id.*

296. *Id.*; *see also supra* note 293 and accompanying text (noting that the legislative history of the CFAA indicates an intent to include the full costs to the victim within the definition of "loss").

297. Over the past few years, the venerable doctrine of trespass has been given new life in modern cyberspace cases. For example, in *eBay, Inc. v. Bidder's Edge, Inc.*, the plaintiff, eBay brought suit against Bidder's Edge for using a software robot to access and gather information contained on the plaintiff's Internet site. 100 F. Supp. 2d 1058, 1060 (N.D. Cal. 2000). eBay operates a publicly accessible auction website where sellers of merchandise list their wares online and the items are then sold to the highest bidder. *Id.*

The defendant, Bidder's Edge, does not provide online auction services in direct competition with eBay, but instead competes indirectly as an online auction aggregator. *Id.* at 1061. Bidder's Edge allows an individual interested in locating information about auctions for a particular type of item to quickly search numerous online auction sites in a single

VI. PRIVATE PROPERTY RIGHTS IN INFORMATION

As the discussion above illustrates, the two elements of a civil action claim—prohibited conduct and loss—rarely pose much of a hurdle for a website owner who seeks to prevent its competitors from accessing and utilizing noncopyrightable information contained on its website. In many ways, it is even easier for a civil action plaintiff to prove that the defendant has violated the CFAA's prohibitions than to prove loss, as plaintiffs have been given surprisingly wide latitude in defining that which constitutes permissible conduct on their web-

---

search, as opposed to performing a separate search on the website of each online auction company. *Id.* at 1061-62. For example, if someone were interested in bidding on a Sammy Sosa baseball card, he or she would want to find out where such auctions were occurring, and more likely than not, the current bid on the baseball card. This data could be obtained by visiting the home page of every online auction site and conducting a search on each one, or by simply conducting one search on the Bidder's Edge site to find out the very same information. *Id.* at 1062.

Bidder's Edge uses software robots to compile the data from individual online auction companies, including the information on eBay's website. *Id.* One may wonder why eBay would object to the additional exposure that a site like Bidder's Edge may bring to eBay's own auctions. The simple fact is that even though eBay may get some publicity, Bidder's Edge also provides information on eBay's direct competitors, potentially informing a consumer about a better deal. *Id.*

Another reason why eBay disapproved of Bidder's Edge's use of software robots on its site is that eBay had been attempting to license such a right to crawl its website to others. *Id.* In fact, prior to filing the lawsuit, eBay and Bidder's Edge had been engaged in licensing negotiations. *Id.* eBay had even consented to Bidder's Edge's robotic activity while negotiations for a formal licensing agreement were underway. *Id.* When, however, the negotiations failed to result in an agreement, Bidder's Edge refused to stop crawling eBay's site. *Id.* Soon thereafter, eBay filed suit against Bidder's Edge alleging a variety of state and federal claims, including common law trespass to chattels and a violation of the CFAA. *Id.* eBay then moved for a preliminary injunction prohibiting Bidder's Edge from accessing its Internet site, to which the court noted that "eBay's motion appears to be, in part, a tactical effort to increase the strength of its license negotiation position and not just a genuine effort to prevent irreparable harm." *Id.* at 1064 n.9.

Despite this fact, the court granted the injunction, ruling only on the trespass claim. *Id.* In order to prevail on the trespass to chattels claim, eBay had to prove that Bidder's Edge had intentionally interfered with eBay's possessory interest in the computer system, and that such conduct had proximately caused damage. *Id.* at 1069-70. However, eBay's computer system had not been harmed in any way by Bidder's Edge's robotic activity. *Id.* at 1064-65. There was no evidence that eBay had suffered any loss of data or that it had experienced any system crashes or slowdowns. *Id.*

But the court surprisingly still found that the element of harm had been satisfactorily demonstrated by eBay. *Id.* at 1069. The court ruled that if Bidder's Edge's "activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." *Id.* at 1066. Therefore, based on the mere possibility of future harm by unidentified third parties, the court enjoined Bidder's Edge's robots from crawling eBay's publicly accessible website. *Id.* at 1069, 1073.

sites.[298] As detailed below, this is due in part to the way in which the statute was drafted, but also how the courts have interpreted the CFAA's provisions.

A. The Constitutional Boundaries of Congressional Power

The original drafters of the CFAA purposely defined the types of acts that would violate the statute rather broadly.[299] Legislators were concerned that if they did otherwise, they would have to regularly amend the CFAA to keep up with the ever changing nature of computer crime, owing to advancements in computer technology.[300] Although this has proven at times to be an attribute of the statute, it has also resulted in conduct falling within the literal language of the statute that Congress, arguably, never intended to be regulated by the Act, such as the access and use of publicly accessible factual information.[301]

Furthermore, it is highly unlikely that Congress even has the power to create private property rights in factual information. Article I, Section 8, Clause 8, of the Constitution, also known as the Intellectual Property Clause, is the source of Congress's power to enact copyright legislation.[302] The same clause in the Constitution that allows Congress to enact copyright legislation to protect "original works of authorship" also restricts the power of Congress to create exclusive rights in information.[303] Congress cannot constitutionally recognize private rights in raw facts.[304] In *Graham v. John Deere Co.*,[305] the Supreme Court stated that in exercising its powers under the Intellectual Property Clause, Congress "may not overreach the restraints imposed

---

298. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000) (holding that the defendant's use of a software robot constituted unauthorized access under the CFAA).

299. *See* S. REP. No. 104-357, at 5 (1996) (noting that the original drafters of the CFAA chose to address the problem of computer crime in a single statute, "rather than identifying and amending every potentially applicable statute affected by advances in computer technology").

300. *Id.*

301. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 346 (1991) (holding that copyright protection does not extend to factual information).

302. U.S. CONST. art. I, § 8, cl. 8 (authorizing Congress "[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").

303. *See id.*; *see also* Yochai Benkler, *Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information*, 15 BERKELEY TECH. L.J. 535 (2000).

304. *Id.* at 544 (citing *Feist*, 499 U.S. at 351).

305. 383 U.S. 1 (1966).

by the stated constitutional purpose."[306] The Court further explained that the Intellectual Property Clause requires Congress to act only in situations where the extension of an exclusive right promotes "[i]nnovation, advancement, and . . . add[s] to the sum of useful knowledge."[307] Congress is therefore prohibited from enacting legislation that encloses or burdens access to information or knowledge already available in the public domain.[308] These limitations reflect a substantive concern towards granting anyone exclusive rights to control and benefit from ideas or facts.[309]

Additionally, Congress cannot bypass the restrictions of the Intellectual Property Clause by enacting legislation to protect works that lack originality under a separate provision of the Constitution, such as the Commerce Clause.[310] Decisions in cases such as *Feist*, which are so heavily based on the constitutionally protected status of public access to facts and information, in essence would be rendered meaningless if limitations on Congress's power under the Intellectual Property Clause could so easily be avoided.[311] The only case to address directly an Intellectual Property Clause challenge to legislation passed under the guise of Congress's Commerce Clause power, supports such an interpretation.[312] In *United States v. Moghadam*,[313] the Eleventh Circuit held that there are "circumstances . . . in which the Commerce Clause cannot be used by Congress to eradicate a limitation upon Congress in another grant of power."[314] In so doing, the court recognized that Congress's power to create intellectual property-like rights under the Commerce Clause is limited by the substantive constraints imposed by the Intellectual Property Clause on the enactment of such rights.[315] These constraints would of course include the requirement of originality, which as explained above, is clearly missing in the case of factual information.[316]

Even in the unlikely situation that Congress could enact legislation that extends copyright-like protection to factual information in compliance with the substantive requirements of the Intellectual

306. *Id.* at 6.
307. *Id.*
308. Benkler, *supra* note 303, at 543.
309. *Id.* at 543-44.
310. *Id.* at 547-48.
311. *Id.* at 545.
312. *Id.* at 546.
313. 175 F.3d 1269 (11th Cir. 1999).
314. *Id.* at 1280.
315. *See id.* at 1280-81; Benkler, *supra* note 303, at 547-48.
316. *See supra* Part II (discussing the requirements for copyright protection).

Property Clause, the private rights would still be subject to First Amendment review.[317] Although the government's intent may not be to suppress speech, nonetheless such a restriction must be shown to serve an important state interest and that "the incidental restriction on alleged First Amendment freedoms is not greater than is essential to the furtherance of that interest."[318] Such a review must take into account the Supreme Court's conclusion that intellectual property rights do not conflict with the First Amendment precisely because of the requirement of originality and the doctrine of fair use.[319] All of this suggests that courts should review with particular care legislation that creates exclusive rights in information without adhering to these fundamental principles.[320]

Furthermore, courts could, and in fact should, interpret the CFAA to avoid such constitutional issues. Under the canon of constitutional avoidance, when "a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, [a court's] duty is to adopt the latter."[321] The avoidance canon rests upon the judicial

---

317. Benkler, *supra* note 303, at 552.

318. United States v. O'Brien, 391 U.S. 367, 377 (1968); *see also* Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 189 (1997); Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 741 (1996); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 662 (1994); Benkler, *supra* note 303, at 556, 588-89.

Commentators have differed as to the appropriate level of review to apply to legislation that creates private rights in information, namely whether such a law is content-based, subjecting it to heightened scrutiny, or content-neutral, thus requiring a lesser, intermediate-level of review. *See* C. Edwin Baker, *First Amendment Limits on Copyright*, 55 VAND. L. REV. 891, 922 (2002) (contending that "copyright laws involve content-based suppression of speech in the simplest and most direct sense"); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 186 (1998) (stating that it is "incorrect to argue that intellectual property law is content-neutral and should therefore be subject to laxer rules [, thus,] [c]opyright liability turns on the content of what is published"); Benkler, *supra* note 303, at 555-56 (observing that general information-control rules are content-neutral, not content-based, as their purpose is the promotion of speech generally, not of one particular speech determined by content). In the case of the CFAA, it would appear that the law is content-neutral as its protections extend to all information, not particular types of information. If this position is incorrect and the CFAA could instead be characterized as a content-based regulation, this would make the statute even more constitutionally suspect.

319. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985); *see also* Benkler, *supra* note 303, at 588. The doctrine of fair use in copyright law, for example, allows an individual to utilize protected portions of another's work without permission, for such things as public commentary, criticism, or parody. *Harper & Row Publishers, Inc.*, 471 U.S. at 547 n.2.

320. *See* Benkler, *supra* note 303, at 588 (discussing constitutional review of legislation creating rights similar to intellectual property rights).

321. Harris v. United States, 536 U.S. 545, 555 (2002) (quoting United States *ex rel.* Attorney Gen. v. Delaware & Hudson Co., 213 U.S. 366, 408 (1909)).

branch's "respect for Congress, which [courts assume] legislates in the light of constitutional limitations."[322] Unfortunately, in recent cases involving the CFAA, courts instead have construed the Act in such a way as to make it constitutionally suspect.[323]

B. Delineating the Proprietary Rights of Website Owners

Courts consistently have granted website owners the exclusive right to regulate the terms upon which access is granted to their publicly available Internet sites, as well as the manner in which any non-copyrightable information contained therein is utilized.[324] The typical review of a website owner's terms is best illustrated by the *Register.com* court's conclusory statement in connection with its cursory analysis of Register.com's CFAA claim: "[B]ecause Register.com objects to Verio's use of search robots they represent an unauthorized access to the [contact information] database."[325] Courts evaluating CFAA claims have not limited the manner in which website owners exercise the power to exclude. Although such a power may be a fundamental right of a property owner,[326] it is not absolute.[327] For example, "[t]he owner of real property has never held an unrestricted right to exclude strangers or regulate activity upon its premises."[328] Instead, the contours of the "relationship[ ] between landowners and those [either] seeking entry to or already present" upon another's land have historically been refined by the common law.[329]

> In fact, the Second Restatement of Torts contains more than twenty sections [that relate to] "privileged" entries onto land over the owner's objections. These include: . . . entry to abate a private nuisance[,] . . . entry by a traveler on a public highway that has become impassable to enter neighboring

---

322. *Id.* at 556 (quoting Rust v. Sullivan, 500 U.S. 173, 191 (1991)).

323. *See infra* Section V.B (questioning the constitutionality of courts' interpretation of the CFAA).

324. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1073 (N.D. Cal. 2000) (granting an injunction based on unauthorized access where the defendant accessed eBay's website in violation of the plaintiff's Terms of Use).

325. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000).

326. Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (characterizing the right to exclude as one of the most essential sticks in a property owner's bundle of rights).

327. Curtis J. Berger, Pruneyard *Revisited: Political Activity on Private Lands*, 66 N.Y.U. L. REV. 633, 667 (1991).

328. *Id.* Blackstone wrote that the right of property must be exclusive, with every entry onto land without the owner's permission amounting to a trespass or transgression; he qualified this statement, however, by listing numerous situations in which entry onto land was in fact permissible. 3 WILLIAM BLACKSTONE, COMMENTARIES *209.

329. Berger, *supra* note 327, at 667.

> land to continue his or her journey[,] and entry because of private necessity.[330]

Additionally, in the case of a publicly accessible website, the owner has already opened its "land" to the general public.[331] This occurs when the website owner chooses to post uncopyrightable information to an Internet site that can be viewed by virtually anyone with an Internet connection. As such, it should be expected that by doing so, the owner of a publicly accessible website relinquishes some of the autonomy owners of private property might traditionally enjoy.[332] Instead, courts have, to some extent, automatically granted legal recognition to the restrictions of website owners without considering the effect on society.[333]

Allowing owners of publicly accessible websites to utilize the CFAA to enforce restrictions placed on access to and use of uncopyrightable information alters the balance of rights struck by copyright law. Copyright seeks to provide sufficient protection to authors, so that they have incentives to create.[334] This is balanced, however, by the primary objective of copyright law, namely to ensure society's access to copyrighted works in order to "promote the Progress of Science and useful Arts."[335]

However, courts interpreting the CFAA have unconstitutionally allowed website owners to unilaterally change this balance to their advantage. Website owners have successfully used the statute to enclose information that belongs in the public domain.[336] In so doing, these website owners are not just hindering their competitors, but negatively affecting society as well. By restricting their competitors' access to and use of this uncopyrightable information, these website owners

---

330. *Id.* The notes to section 197 contain fifteen examples of private necessity, including a passerby that enters a private dwelling after hearing screams of distress from inside and an aviator that is forced to make an emergency landing on another's field. *Id.* at 667 n.198 (discussing the Section 197 illustrations).

331. *See* Berger, *supra* note 327, at 652-57 (distinguishing between truly private places, such as the home, and public spaces, like shopping centers). *But see* Lloyd Corp. v. Tanner, 407 U.S. 551, 569 (1972) (declaring that property does not "lose its private character merely because the public is generally invited to use it for designated purposes"). However, as discussed *infra*, an argument can be made that the holding of this case should be narrowly construed.

332. Berger, *supra* note 327, at 636.

333. *See* Luh, *supra* note 98 (suggesting that preventing access to publicly accessible content "threatens the openness of the Internet").

334. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 449 U.S. 340, 349-50 (1991).

335. *Id.* at 349; U.S. CONST. art. I, § 8, cl. 8.

336. Elkin-Koren, *supra* note 12, at 180-82 (discussing eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000)).

are denying the public the benefits that accrue from increased competition in the marketplace.[337]

Furthermore, the enforcement of a website owner's restrictions on data contained on a publicly accessible website undermines the balance struck between copyright law and the First Amendment.[338] Utilization of the CFAA to enforce a website owner's restrictions on publicly available factual information results in the enclosure of the public domain with a shift in the legal status of information that is not caused by the absence of government regulation.[339] Instead, it is the result of a governmental decision that such restrictions are enforced and it "is no less and no more a regulatory decision than the decision not to enforce them."[340] As such, the First Amendment's injunction that "Congress shall make no law" is engaged, and any legislation that directly regulates information production and exchange must be shown to serve an important government interest without restricting substantially more speech than necessary.[341] Although protecting the integrity of computer systems and confidential information may qualify as a laudable legislative goal, the CFAA's provisions as drafted and interpreted by the courts are significantly more restrictive of speech than necessary to serve these interests.

The fact that the information collected and utilized by software robots would most likely be characterized as "commercial speech" as opposed to "non-commercial speech" does not alter this conclusion.[342] The U.S. Supreme Court has ruled that society has a right to receive commercial speech.[343] In *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.*,[344] the Court stated,

> So long as we preserve a predominantly free enterprise economy, the allocation of our resources in large measure will be made through numerous private economic decisions. It is a matter of public interest that those decisions, in the aggre-

---

337. *Id.* at 182.

338. *See* Benkler, *supra* note 176, at 358 (asserting that "[e]nclosure . . . conflicts with the First Amendment injunction that government not prevent people from using information or communicating it").

339. *See id.* at 359-60 (discussing enacted and proposed legislation that is part of the "enclosure movement," including the Digital Millennium Copyright Act, Article 2B (now UCITA), and the Collections of Information Antipiracy Act). *See generally* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 (1998).

340. Benkler, *supra* note 176, at 433.

341. *Id.* at 394, 413.

342. *See* Va. St. Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 765-66 (1976) (applying intermediate scrutiny to state restrictions on commercial speech).

343. *Id.* at 765.

344. 425 U.S. 748 (1976).

> gate, be intelligent and well informed. To this end, the free flow of commercial information is indispensable.[345]

Additionally, the Court recognized that

> [a]s to the particular consumer's interest in the free flow of commercial information, that interest may be as keen, if not keener by far, than his interest in the days most urgent political debate . . . . Therefore, even if the First Amendment were thought to be primarily an instrument to enlighten public decisionmaking in a democracy, we could not say that the free flow of information does not serve that goal.[346]

Despite the Supreme Court's recognition of the importance of First Amendment interests, the Court has not always held that private property owners must give way to such rights.[347] In a series of cases, the Supreme Court has vacillated on the proper balance between First Amendment rights and private property rights. In *Amalgamated Food Employees Union Local 590 v. Logan Valley Plaza, Inc.*,[348] the Supreme Court held that picketing on the sidewalks and a parking lot adjacent to a non-union store by local union members could not be enjoined by the shopping center because it would be an impermissible constraint on the protestors' First Amendment rights.[349] But four years later in *Lloyd Corp. v. Tanner*,[350] the Court overruled *Logan Valley*, holding that the First Amendment does not prevent a private shopping center owner from prohibiting the distribution of leaflets protesting the Vietnam War on its premises.[351] Lastly, in *Pruneyard Shopping Center v. Robins*,[352] the Supreme Court held that a state did not violate a property owner's First and Fifth Amendment rights by granting individuals the right to enter a privately owned shopping center and gather petitions.[353]

In attempting to reconcile these various opinions, it is important to keep in mind that in balancing private property interests against constitutional rights, the Court weighs the effect of any expressive ac-

---

345. *Id.* at 765.

346. *Id.* at 763, 765 (footnotes omitted).

347. *E.g.*, Lloyd Corp. v. Tanner, 407 U.S. 551, 570 (1972) (holding that a privately owned shopping center that allowed public access was not dedicated to the public use for the exercise of political speech).

348. 391 U.S. 308 (1968).

349. *Id.* at 325.

350. 407 U.S. 551 (1972).

351. *Id.* at 570.

352. 447 U.S. 74 (1980).

353. *Id.* at 88; *see also* Berger, *supra* note 327, at 633-94 (evaluating *Pruneyard* and arguing for recognition of free speech right in shopping malls).

tivity, as well as the attendant public benefit.[354] In the case of a website owner attempting to use the CFAA to prevent a software robot from accessing and utilizing uncopyrightable information posted on an Internet site, the balance clearly should be struck in favor of First Amendment rights. The software robot is collecting data that is not constitutionally entitled to protection.[355] It is information that cannot be owned by any one party, as it is part of the public domain.[356] Additionally, in most instances the data provides the basis for more effective competition against the website owner.[357] Despite the website owner's views to the contrary, such competition is desirable.[358] As discussed above, the public benefits from a marketplace with increased options.[359]

Furthermore, to the extent that a software robot occupies a portion of the website owner's computer server, the intrusion is minimal.[360] The software robot does not interfere with a potential customer's ability to access information on the website owner's Internet site, as both entities can do so simultaneously.[361] Additionally, unlike picketing or the gathering of petitions on private shopping mall property, a software robot's expressive activity does not cause any disruption to commercial business occurring on the website.[362] Also, the typical software robot causes absolutely no harm to the website owner's computer system or the integrity of the data contained therein.[363]

The CFAA as currently drafted and interpreted by recent court decisions grants too much proprietary control to website owners at the public's expense.[364] These decisions upset the careful balance of rights that the Copyright Act has struck between authors and society.[365] Using this power, these owners of publicly accessible Internet

---

354. *See Pruneyard*, 447 U.S. at 88; *see also* O'Rourke, *supra* note 18, at 619; Berger, *supra* note 327, at 678-84.

355. Facts are not entitled to protection because they are not "original." Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 347 (1991).

356. *Id.* at 347-48.

357. Elkin-Koren, *supra* note 12, at 182.

358. *Id.*

359. *See supra* Part IV.

360. O'Rourke, *supra* note 18, at 565.

361. *Id.* at 565-66.

362. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063 (N.D. Cal. 2000) (noting that while the defendant's robot accessed eBay 100,000 times daily, the defendant's queries only constituted at most 1.53% of total daily requests).

363. Luh, *supra* note 98.

364. Elkin-Koren, *supra* note 12, at 182.

365. *See* Benkler, *supra* note 176, at 386-94 (discussing the relationship between copyright law and the First Amendment).

sites have attempted to stifle the free flow of information in order to prevent legitimate competition that could effect their bottom line.[366] To the extent that relief from truly harmful robotic activity is warranted, the CFAA is not the appropriate vehicle for providing redress.

VII. AN AMENDMENT AND AN ALTERNATIVE TO THE CFAA

As discussed above, the CFAA was never designed to protect information contained on publicly accessible websites.[367] Furthermore, court interpretations that allow for the protection of facts in such cases are constitutionally suspect.[368] Instead, the statute was promulgated to provide relief to true victims of hacking, parties whose computer systems or confidential data actually had been compromised.[369] In order to ensure that the CFAA is properly utilized in the future, the statute needs to be amended.

Earlier it was noted that all fifty states have some form of computer crime legislation.[370] In detailing the various offenses, two states, namely Louisiana and Mississippi, include identical provisions which provide that the criminal statute does not apply to "disclosure, use, copying, taking or accessing by proper means."[371] The term "proper means" is defined in part as "observation of the property in public use or on public display."[372]

Similar language could be added to the CFAA to ensure that software robots can access and utilize information on publicly availa-

---

366. Elkin-Koren, *supra* note 12, at 182.

367. *See supra* Part III.

368. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349-50 (1991) (explaining that the Intellectual Property Clause offers copyright protection for original works, not unoriginal facts).

369. *See, e.g.*, Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 42 U.S.C. § 13701 (2000)) (adding a civil remedy provision to the CFAA).

370. *See supra* note 59 (providing a comprehensive list of state computer crime legislation).

371. LA. REV. STAT. ANN. § 14:73.2 (West 1997 & Supp. 2003); MISS. CODE ANN. § 97-45-9 (2001).

372. LA. REV. STAT. ANN. § 14:73.1(11) (West 2001); MISS. CODE ANN. § 97-45-1(k) (1994 & Supp. 2003). The full definition as provided in Mississippi's statute is as follows:

> (k) "Proper means" includes:
>
> (i) Discovery by independent invention;
>
> (ii) Discovery by "reverse engineering"; that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must be by lawful means;
>
> (iii) Discovery under license or authority of the owner;
>
> (iv) Observation of the property in public use or on public display; or
>
> (v) Discovery in published literature.

Id.

ble websites without violating the Act. The civil action provision[373] could be amended with the following language:

> No action may be brought under this subsection for the disclosure, use, copying, taking, or accessing of a computer to obtain information on public display.

Further, "public display" could be defined as follows:

> The term "public display" includes information available to the public without a fee, including information on publicly accessible Internet websites.

Although this exemption would apply to both copyrightable and uncopyrightable information, a copyright owner would not be prevented from utilizing the copyright laws to obtain relief where warranted.

This proposed change to the CFAA is not meant to suggest that an owner of a publicly accessible Internet site is completely without a remedy. However, the proper theory upon which relief may be granted must appropriately balance the website owner's proprietary rights with the public benefit that ensues from the free flow of information. Dan Burk has suggested a modified version of the common law claim of nuisance as an alternative to website owners' trespass actions, but it would also appear to be an acceptable substitute for a CFAA claim.[374] This is due to the fact that such a cause of action lies only if the cost of the intrusive conduct outweighs the benefit.[375] Burk explains that "the 'muddy' nature of nuisance would allow computer owners on the Net to exclude unreasonably costly use of their servers, while allowing access for socially beneficial uses, even if the server owner might otherwise object."[376]

Certainly a website owner would still have the option of physically disconnecting from the Internet to avoid any undesirable uses, but doing so would also result in the loss of the attendant benefits of being part of such a network.[377] However, as Burk points out, "proper application of the nuisance standard would make this drastic action unattractive on average to rational server owners."[378] Instead, website owners more likely will tolerate the occasional "unwelcome" visitor or "undesirable" use in order to take advantage of the commercial exposure that the placement of a website on the Internet brings. A remedy

---

373. 18 U.S.C. § 1030(g) (2003).

374. *See* Burk, *supra* note 255, at 53-54 (discussing digital nuisance as an alternative to trespass actions).

375. *Id.* at 53-54.

376. *Id.* at 53.

377. *Id.*

378. *Id.*

such as digital nuisance, therefore, would recognize that a website owner has some limited proprietary rights in its Internet site, but ensure that those rights are not exercised to the public's detriment.

VIII. CONCLUSION

The CFAA was enacted to provide protection from incidents of computer hacking.[379] Despite recent court decisions suggesting the contrary,[380] the statute was never intended to afford website owners with a method for obtaining absolute control over access to and use of information they have chosen to post on their publicly accessible Internet sites. Additionally, such sweeping interpretations of the CFAA threaten the continued openness of the Internet and competition in the marketplace to the public's detriment.[381] The CFAA, therefore, needs to be amended to ensure that only those entities that have suffered the type of harm for which the statute was designed obtain relief. Hopefully this will also encourage courts, when faced with similar types of claims in the future, to strike a more proper balance in rendering decisions on the proprietary rights of website owners.

379. S. REP. NO. 104-357, at 3-5 (1996).

380. *E.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000) (enjoining Verio from using a web robot to access publicly available factual information on Register.com's website).

381. Elkin-Koren, *supra* note 12, at 181-82.