

SYRACUSE JOURNAL OF LAW AND TECHNOLOGY

How Much Protection is Too Much: Using the Computer Fraud and Abuse Act as an Appropriate Means to Protect Compilations of Data

James A. Tanner

INTRODUCTION

Hooray, the digital age is here. All we have to do now is carve out our little corner of the information industry and wait for the revenues to come rolling in. It's all part of the American dream, right? Gather information and get rich. However, protection of information invaluable to others, thus withheld, could stymie competition creating a virtual monopoly on information. But how much protection should we allow to compilers of information? How much protection is reasonable or desirable?

By way of illustration, imagine an entrepreneur that creates a movie index, Moviedex, listing every movie ever produced alphabetically according to subject matter, perhaps including a cross reference pertaining to lead actors/actresses as well. The compilation of this index represents a substantial effort and expense undertaken by its creator. He uploads his creation onto the internet and charges a user fee for access. Video rental and retailers are interested and subscribe to his service. After six months, his subscribers decline to renew because a new website containing the same information has appeared and costs less. After investigation, our entrepreneur discovers that a competitor has copied his entire index and can charge less for access since creation was less expensive. After speaking with an attorney, our entrepreneur discovers the copying was perfectly legal and there was really nothing he could do to protect his Moviedex compilation. Disgruntled, he incurs a substantial financial loss and discontinues

service.

The issue of data protection is not new. There have been debates in the United States, and countries around the world, pertaining to the amount of protection desirable for data compilations. After all, the compiler presumably has gone through the trouble of creating his product. Why shouldn't he receive protection for the fruits of his labor? According to John Locke, a man is privileged to the fruits of his own labor.¹ He expended the time and energy involved in creation, thus he deserves to call it his own.²

In contrast to this view, however, is the interest of society as a whole to free access to information. Without an informed, educated society, where would we be? Probably still trying to invent the wheel. Without free access, those who propose to commodify information would lack the requisite availability needed to compile their product. Likewise, the scientific and technological industry would suffer because invention and creation go hand in hand with the dissemination of valuable information and ideas.

As more and more people rely on technology to facilitate the compilation and storage of data, it seems evident that a substantial gap exists pertaining to competing legal theories striving to protect the rights of owners in their data compilations. Although attempts at universal international law have been made to remedy the disparity, the persistence of the problem remains.

The United States, and the rest of the world in general, have traditionally looked to the doctrine of copyright for protection of data compilations. Although providing slim coverage for data compilations, through creative selection and arrangement, some protection was available while taking into account the information consumer's right to access. Thus, protection was

¹ JOHN LOCKE, THE SECOND TREATISE OF CIVIL GOVERNMENT § 27 (1690).

² *Id.*

slight, but it existed.

By enacting the Database Directive, the European Community has raised the bar on database protection.³ Rather than balancing the right to access with the right to protect, the Directive leans dramatically in favor of database owners and compilers essentially granting a monopoly on information.⁴

Rather than focusing on protecting data compilations through creative selection and arrangement or “sweat of the brow”⁵, however, we should concentrate on the damages incurred for the misappropriation, misuse, and damages resulting from the illegal extraction of information from a protected computer. This note focuses on such an approach, through the Computer Fraud and Abuse Act. Part I describes the current schemes for protection of data compilations in the United States and proposals submitted to Congress to strengthen such protection. Part II discusses the relevant international attempts to remedy the dilemma posed by data compilations in the digital age. Part III illustrates the proposal adopted by the European Community that grants a *sui generis*⁶ right to non-creative database compilers if compilation was effected through substantial effort or expense. Part IV will analyze how much protection is

³ See Council Directive 96/9/EC, 1996 O.J. (L 077) 20 [hereinafter EU Directive].

⁴ See *id.*

⁵ The “sweat of the brow” doctrine was a means to protect the interests of data compilers by rewarding the labor involved in creating data compilations. See Amy C. Sullivan, *When the Creative is the Enemy of the True: Database Protection in the U.S. and Abroad*, 29 AIPLA Q.J. 317, 327 (2001) (the purpose of this doctrine was to reward the labor and investment involved in compiling a database and was based on the natural law concept that individuals are entitled to the fruits of their labor); see also MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW 69-71 (3d ed. 1999).

⁶ This right creates a new regime of legal protection for data compilations that does not exist in traditional U.S. approaches of misappropriation or copyright law. See Jane C. Ginsburg, *Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad*, 66 U. CIN. L. REV. 151, 171 (1997) (*sui generis* right encompasses substantial investment made by database producers); see also Michael Freno, *Database Protection: Resolving the U.S. Database Dilemma with an Eye Toward International Protection*, 34 CORNELL INT’L L.J. 165, 183 (2001) (explaining scope of *sui generis* right as protection which applies to collection of independent works or data, which database maker qualitatively or quantitatively made substantial investment in acquiring, substantiating, or presenting contents).

needed, or appropriate, for non-creative data compilations. Finally, Part V discusses a proposed solution to the problem concerning protection of non-creative data compilations.

I. CURRENT AND PROSPECTIVE U.S. LAW ESPOUSING PROTECTION FOR DATA COMPILATIONS.

Law in the United States does not provide broad protection for data compilations due to an interpretation of the Constitution by the Supreme Court supporting a policy favoring free access to disclosed data.⁷ This policy, according to the Court, is grounded within both the constitution and the federal copyright statute as enacted by Congress in 1976.⁸ The intent is to maintain a balance between the author's incentive to create, fostering the promotion of science and the useful arts, and the free access to facts and information necessary to sustain our informed, educated society.

Congress established limited protection to compilations of data under the 1976 Copyright Act by extending copyright only to material contributed by the author of the work, not the pre-existing material employed in the work.⁹ Additionally, copyright protection does not extend to a work where any preexisting material contained therein has been used unlawfully.¹⁰ Therefore, the misappropriation of another's work, or use without authorization, may render the entire compilation unprotectable.¹¹

In *Feist Publications v. Rural Telephone Service Co.*, the Supreme Court limited the

⁷ *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991); Jane C. Ginsburg, *No "Sweat"?: Copyright and Other Protection of Works of Information After Feist v. Rural Telephone*, 92 COLUM. L. REV. 338, 339 (1992).

⁸ Ginsberg, *supra* note 7.

⁹ 17 U.S.C. § 103(b) (2000).

¹⁰ 17 U.S.C. § 103(a) (2000).

¹¹ *Id.*

scope of copyright protection in data compilations even further.¹² Although compilations of facts and data are protectable, the facts and ideas themselves are not.¹³ The rationale for denying protection to ideas or facts one narrates is that facts “do not owe their origin to an act of authorship.”¹⁴ Consequently, the Court refused to extend copyright protection to telephone white pages published by a local telephone company.¹⁵ As such, *Feist*, the publisher of a regional telephone directory, was not held liable for copyright infringement for copying over 1,300 listings from Rural’s white pages.¹⁶ The Court’s reasoning, stated in the opinion by Justice O’Connor, was that the white pages published by Rural lacked the requisite originality requirement deemed essential under the statute.¹⁷

The Court determined that an element of originality is required to establish copyright protection.¹⁸ Originality does not denote novelty or innovation, but that the “work was independently created by the author... and that it possesses at least some minimal degree of creativity.”¹⁹ Therefore, a compilation of facts, not themselves copyrightable, must be selected and arranged in such a way as to create a work original to the particular author.²⁰ “The requisite level of creativity for factual compilations is extremely low, but it does exist.”²¹

¹² *See Feist*, 499 U.S. at 340.

¹³ *Id.* at 344.

¹⁴ *Id.* at 347.

¹⁵ *Id.* at 364.

¹⁶ *Feist* 499 U.S. at 362.

¹⁷ *Id.*

¹⁸ *Id.* at 345.

¹⁹ *Id.*

²⁰ *Id.* at 348.

²¹ *Feist*, 499 U.S. at 345.

Through this originality requirement, the Supreme Court effectively eliminated the “sweat of the brow” doctrine that typically espoused rights under a form of labor theory.²² Through the “sweat of the brow” doctrine, previous courts had handed out proprietary interests in facts.²³ Consequently, future authors could not save valuable time and effort by copying facts from a prior work; they must essentially start from scratch and recompile.²⁴ Such “reinvention of the wheel” leads to waste. In fact, it was just such wasted effort the Court addressed when proscribing the copyright of ideas and facts.²⁵ After all, the objective of copyright is not to reward the labor of authors, but to promote the progress of science and the useful arts.²⁶

In the wake of *Feist*, Congress feared that private businesses would refuse to create data compilations that could benefit the public due to the inability to adequately protect their investment, thus several attempts have been made to strengthen copyright protection of data compilations.²⁷ Although several attempts have been made, primarily in the House, no bill has effectively passed both houses of Congress for presidential approval.

By introducing House Bill 3531, Representative Moorhead proposed to amend title 15 of the United States Code to promote investment and prevent intellectual property piracy with respect to databases.²⁸ The Database Investment and Intellectual Property Anti-Piracy Act of 1996 was introduced to resurrect the “sweat of the brow” doctrine that *Feist* had eliminated by

²² *Id.* at 352.

²³ *Id.* at 353-54.

²⁴ *Id.*

²⁵ *Id.* at 354.

²⁶ *Id.* at 349.

²⁷ Michael Freno, Note, *Database Protection: Resolving the U.S. Database Dilemma with an Eye Toward International Protection*, 34 CORNELL INT’L L.J. 165, 167 (2001).

²⁸ Database Investment and Intellectual Property Anti-Piracy Act of 1996, H.R. 3531, 104th Cong. (1996).

protecting data compilations created through substantial investment of human, technical, or financial resources.²⁹ By creating a form of sui generis property protection to provide compilers of non-original databases some amount of security, Representative Moorhead intended a novel reconfiguration of current American intellectual property law.³⁰ Rather than the promotion of science and the useful arts, the sui generis right appears to promote the economic well being of the information compiler.³¹ This protection would broaden the rights of the data compiler while restricting the current rights or exemptions enjoyed by information consumers through copyright.³²

The Collection of Information Anti-Piracy Act, House Bill 2652, was intended to protect against the misappropriation of collections of information by penalizing any person who extracts or uses in commerce a substantial part, measured quantitatively or qualitatively, of a collection of information maintained by another person.³³ According to representative Howard Coble, Chairman of the Subcommittee on Courts and Intellectual Property, this bill would “fill the void fashioned by the Supreme Court in our intellectual property system.”³⁴ It would strike a balance ensuring adequate protection for companies to invest in the development of information compilations without inhibiting the scientific and research communities.³⁵ Instead of relying

²⁹ H.R. 3531, 104th Congress § 3(a) (1996).

³⁰ Peter Jaszi, *Summary and analysis of H.R. 3531*, available at <http://arl.cni.org/info/frn/copy/peter.html> (last visited Feb. 1, 2003).

³¹ Jaszi, *supra* note 30.

³² *Id.*

³³ Collection of Information Anti-Piracy Act, H.R. 2652, 105th Cong. (1997).

³⁴ *Collection of Information Anti-Piracy Act: Hearings on H.R. 2652 Before the Subcomm. on Courts and Intellectual Property*, 105th Cong. 1-2 (1998) (statement of Chairman Howard Coble).

³⁵ Hearings on H.R. 2652, *supra* note 34, at 2.

solely on copyright protection, the Act relies on unfair competition principles to prevent misappropriation of another's information.³⁶ Thus, the Act proposed to add a chapter entitled "misappropriation of collections of information" to the Copyright Act focused on protecting non-original compilations of data.³⁷

In 1999, Representative Coble introduced further legislation into the House of Representatives to amend the Copyright Act to protect certain collections of information.³⁸ The Collection of Information Anti-Piracy Act, House Bill 354, was proposed to protect owners of data compilations from those who sought to profit by extracting or making available to others information gathered through the investment of substantial monetary or other resources.³⁹ Like House Bill 2652, 354 proposed to amend the Copyright Act by adding a chapter entitled "collections of information."⁴⁰ The primary difference between House Bill 354 and its predecessor, 2652, is that 354 allowed for a fair use exception and limits protection to fifteen years.⁴¹

Through the Consumer and Investor Access to Information Act, House Bill 1858, Congress meant to prevent the wholesale misappropriation of databases.⁴² The Bill prohibited the sale in interstate commerce of data compilations that have been duplicated from another database that was collected and organized by another person or entity when such a copy was

³⁶ *Id.*

³⁷ Collection of Information Anti-Piracy Act, H.R. 2652, 105th Cong. (1997).

³⁸ Collection of Information Anti-Piracy Act, H.R. 354, 106th Cong. (1998).

³⁹ Collection of Information Anti-Piracy Act, *supra* note 38, at § 1402.

⁴⁰ *Id.* at § 2.

⁴¹ *Id.*; *see also* Freno, *supra* note 27, at 175.

⁴² Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. (1999); Freno, *supra* note 27 at 176.

intended to compete with the original creator.⁴³ However, to violate House Bill 1858, the infringing party must create a database substantially similar to the compilation allegedly copied.⁴⁴

The Senate also tried to increase protection in data compilations by promoting S. 2291, guaranteeing similar protection to H.R. 2652, specifically the prohibition on extraction or use in commerce of a substantial part, measured quantitatively or qualitatively, of a collection of information gathered or maintained by another through investment of substantial resources so as to cause harm to the actual or potential market of that person.⁴⁵

Copyright has the potential to protect data compilers in the fruits of their labor if a creative spark can be identified.⁴⁶ However, protection will be afforded only to original material contributed by the author, not to preexisting material contained therein or facts or ideas.⁴⁷ As stated previously, the threshold of originality is low, but it does exist.⁴⁸

Nonetheless, a category of works remains that will not qualify for copyright protection because there is no creative spark whatsoever or it is so trivial as to be virtually nonexistent.⁴⁹ If one of the abovementioned bills, or something similar, makes it through Congress, then compilers of non-creative databases will have a means to protect their economic expenditure of labor. Unfortunately, passage of the above bills could encounter problems of their own, such as

⁴³ Consumer and Investor Access to Information Act of 1999, H.R. 1858, 106th Cong. (1999).

⁴⁴ *Id.* at § 102.

⁴⁵ Collection of Information Anti-Piracy Act, S. 2291, 105th Cong. (1997).

⁴⁶ *See Feist*, 499 U.S. 340.

⁴⁷ *Id.* at 352.

⁴⁸ *Id.* at 362.

⁴⁹ *Feist*, 499 U.S. at 359.

constitutional issues dealing with the advancement of science and the useful arts or conflicting statutory authority, such as the Freedom of Information Act.⁵⁰

Referring back to our Moviedex entrepreneur, the selection and arrangement of the movie titles will likely fail the *Feist* test. Alphabetical listing under a topical heading will likely be viewed similarly to Rural's white pages. There is nothing remotely creative about listing an index alphabetically.⁵¹ Even the cross reference to actors/actresses will likely not save the analysis. Thus, although copyright remains a competent doctrine to protect authors of creative work, it is not an appropriate means to protect non-creative data compilations. Protection will have to be sought elsewhere.

When Congress enacted the Computer Fraud and Abuse Act (CFAA), it created another prospective means by which compilations of data could be protected.⁵² The intent of Congress, however, was somewhat different. The CFAA was originally enacted with the intention of protecting national security related information.⁵³ However, as the computer industry produced further technological innovations, Congress amended the act to protect computers subject to federal jurisdiction from hackers.⁵⁴

The CFAA is a criminal statute that also provides a private, civil right of action for any violation of its terms.⁵⁵ All that most sections require for protection is that the information is

⁵⁰ 5 U.S.C. § 552 (2000) (amended 2002).

⁵¹ *Feist*, 499 U.S. at 363.

⁵² Michael Levinson & Christopher Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information*, 19 No. 9 COMPUTER & INTERNET LAW 11 (2002); *See generally*, 18 U.S.C. § 1030 (2000).

⁵³ H.R. 4562, 99th Cong., 132 CONG. REC. E1206-01 (1986).

⁵⁴ Pub.L. No. 99-474 § 2, 100 Stat. 1213 (Oct. 16, 1986); H.R. 4562, 99th Cong., 132 CONG. REC. E1206-01 (1986).

⁵⁵ Richard Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 701 PLI/Pat 115, 146 (2002).

stored on a computer.⁵⁶ Furthermore, rather than focusing on an originality requirement to establish protection in the first place, the CFAA focuses on damages, whether they be actual physical damages⁵⁷ or unauthorized access.⁵⁸ Thus, beyond the prohibition of a broad range of hacking, general disruptive and destructive breaches of networks, and the releasing of viruses into computer networks, the CFAA forbids the misappropriation of information contained in electronic databases.⁵⁹

As amended in 1996, the CFAA proscribes intentional unauthorized access, and use that exceeds authorized access, to all protected computers used in international commerce or communications.⁶⁰ To prove a violation of the act, the government must show access or damage to a protected computer intentionally caused by the trespasser's conduct and the harm incurred exceeded five thousand dollars, was a threat to public safety, caused an impairment to medical records, or caused harm to any person.⁶¹ A system is considered damaged when any impairment to the integrity or availability of data, a program, a system or information exists.⁶² Likewise, loss is defined as any reasonable cost 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

⁵⁶ Levinson & Paetsch, *supra* note 52, at 12.

⁵⁷ 18 U.S.C. § 1030(a)(5) (2000).

⁵⁸ 18 U.S.C. § 1030(a)(2) (2000).

⁵⁹ D. Jean Veta & Rochelle Rubin, *Network and Information Security: Domestic and International Initiatives to Combat Cybercrime*, 711 PLI/Pat 955, 968 (2002).

⁶⁰ 18 U.S.C. § 1030(a)(2) (2000); Kirk Ruthenberg, *Chapter 6. Data Security Statutes*, in DATA SEC. & PRIVACY LAW: COMBATING CYBERTHREATS Dataspl S 6:3 (2002).

⁶¹ *Money Laundering Update 2002: What You Need to Know Now*, 1337 PLI/Corp 361, 656 (2002).

⁶² 18 U.S.C. § 1030(e)(8) (2000); Money Laundering, *supra* note 61.

because of the interruption of service.⁶³

The statute provides that “protected computers” shall mean any computer used by the United States government or a financial institution thereof, or which is used in international commerce or communication whether located within the continental United States or not.⁶⁴ Essentially, this provision would include virtually any computer connected to the internet.⁶⁵

Likewise, as defined by statute, “exceeds authorized access” means access to a computer with authorization and to use that access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter.⁶⁶ When access is granted to view the contents of a program or database, such access is restricted by the terms and conditions imposed upon the agreement when it was made. Unless granted the right to change, extract, or copy information, such conduct is beyond the scope of the grant, thus exceeds the authorization contracted.

Punishment under the CFAA may consist of criminal sanctions, monetary damages, injunction, or any combination thereof.⁶⁷ As mentioned previously, the CFAA is a criminal statute that allows for civil claims by those who have suffered loss or damages due to the illegal conduct of the breaching party.⁶⁸ Such damages could be the result of releasing a virus through e-mail, hacking into a protected computer, or something as simple as overloading an internet service provider’s system by sending inordinate amounts of junk advertisements known as

⁶³ 18 U.S.C. § 1030(e)(11) (2000); *United States v. Middleton*, 231 F.3d 1207, 1210 (9th Cir. 2000) (The definition of loss includes a wide range of harms typically suffered by the victims of computer crimes).

⁶⁴ 18 U.S.C. § 1030(e)(2) (2000).

⁶⁵ Ruthenberg, *supra* note 60, at 1.

⁶⁶ 18 U.S.C. § 1030(e)(6) (2000).

⁶⁷ 18 U.S.C. § 1030(c) (2000).

⁶⁸ Lesser, *supra* note 55.

SPAM.⁶⁹

The courts have applied the expansive language of the statute broadly enough to suggest that the CFAA may become a mainstay of civil and criminal litigation protecting computerized information.⁷⁰ Although enacted as a defense against hackers, the CFAA has been applied by the courts in a variety of contexts specifically geared towards the protection of information, whether it be confidential or publicly available information.⁷¹

In *Register.com, Inc. v. Verio, Inc.*, the District Court found that Verio's access to Register.com's website to obtain data for mass marketing purposes was unauthorized in violation of 18 U.S.C. § 1030(a)(2)(C).⁷² Register.com's terms and conditions of use specifically stated that "you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone."⁷³ Verio's e-mails clearly violate Register.com's terms of use.⁷⁴ Consequently, the judge ruled that the unauthorized use of this information has caused and will cause Register.com irreparable damage, thus they are entitled to injunctive relief.⁷⁵

In *E.F. Cultural Travel v. Explorica*, the First Circuit held that a former employee exceeded his authorized access to his former company's website by using proprietary

⁶⁹ Frank Andreano, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem* 27 AM. J. CRIM. L. 81, 94-95 (1999).

⁷⁰ Levinson & Paetsch, *supra* note 52, at 16.

⁷¹ *Id.*

⁷² *Register.com, Inc. v. Verio, Inc.*, 126 F.Supp.2d 238, 253 (S.D.N.Y. 2000).

⁷³ *Id.* at 242.

⁷⁴ *Id.* at 245 n.6.

⁷⁵ *Register.com, Inc.*, 126 F. Supp. 2d at 253.

information to access and organize tour and travel prices from their database.⁷⁶ The court decided that the term loss, clearly derived from Congressional intent, includes remedial expenses borne by the victim other than actual, physical damages to computer or database.⁷⁷ Therefore, since EF Cultural Travel significantly exceeded the statutory five thousand dollar threshold in consulting fees to determine if the website had been compromised, the preliminary injunction imposed by the district court was affirmed.⁷⁸

The CFAA essentially provides victims of computer fraud and data misappropriation with a cause of action that doesn't exist under copyright. Generally speaking, non-creative data compilations are protectable as long as they are stored electronically on a protected computer.⁷⁹ As previously defined, a protected computer is one used in interstate or foreign commerce or communication.⁸⁰ Therefore, since Moviedex is an electronic compilation accessed over the internet, the CFAA would provide our entrepreneur with remedial measures against the competitor if a showing is made that the access was unauthorized or in excess of authorization.

Although the CFAA represents a realistic step forward in protecting non-creative data compilations, without the dangers of fact or idea suppression, there remains the potential to hinder the system of another without actually exceeding authorized access or causing little or no damage. Thus, a supplemental means may be required to protect the medium of expression.

The torts doctrine of Trespass to Chattels is another means of indirectly protecting compilations of data by protecting the forum on which the data is stored. Initially, the doctrine

⁷⁶ E.F. Cultural Travel v. Explorica, 274 F.3d 577, 583 (1st Cir. 2001).

⁷⁷ *Id.* at 585.

⁷⁸ *Id.*

⁷⁹ *See generally* 18 U.S.C. § 1030 (2000).

⁸⁰ 18 U.S.C. § 1030(e)(2)(B) (2000).

of trespass to chattels was used to combat SPAM sent via internet providers.⁸¹ However, the doctrine has been expanded to include the trespass of spiders and robots used to search the internet.⁸² Essentially, the proponents of the trespass to chattels approach want to extend the terms “trespass” and “chattel” to the intangible forum of the internet.⁸³ However, electronic databases appear elsewhere besides the intangible realm of cyberspace. They exist buried within the memory of personal computers that happen to be connected to the internet. In such situations, where the property of another must be encroached to access or withdraw information, the doctrine of trespass to chattels should be invoked.

According to the Restatement of Torts, “one who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if, a) he dispossesses the other of the chattel, or b) the chattel is impaired as to its condition, quality or value, or c) the possessor is deprived of the use of the chattel for a substantial time, or d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.”⁸⁴ Therefore, unless an injury has occurred, trespass to chattels cannot be invoked, whether in cyberspace or your tangible office space.⁸⁵

Although the trespass to chattels doctrine historically has entailed the dispossession or damage of another’s tangible objects, the courts have extended such protection to intangible

⁸¹ See *America Online, Inc. v. National Health Care Discount, Inc.*, 174 F. Supp. 2d 890 (N.D.Ia 2001); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2001); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F.Supp. 1015 (S.D.Oh. 1997); see also Laura Quilter, *The Continued Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L. J. 421 (2002).

⁸² Quilter, *supra* note 81, at 421.

⁸³ *Id.*

⁸⁴ RESTATEMENT (SECOND) OF TORTS § 218.

⁸⁵ See RESTATEMENT (SECOND) OF TORTS § 217, comment a; see also Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117, 154 (2002).

“possessions” such as electronic data and internet websites.⁸⁶ The rationale is that these creations, although intangible, belong to the individual who created them. An injury to one’s property can occur in cyberspace through improper use and trespass just as damage can occur to your BMW through similar means, such as improper maintenance and theft. Likewise, a reasonable person would certainly regard a competitor’s use of his server for the competitor’s profit as seriously reducing its value.⁸⁷

In *eBay v. Bidder’s Edge*, the District Court enjoined Bidder’s Edge from accessing eBay’s website and copying its database using a robot.⁸⁸ The court determined that to prevail on a trespass to chattel claim, involving computer system access, “the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff’s possessory interest in the computer system; and (2) defendant’s unauthorized use proximately resulted in damage to plaintiff.”⁸⁹ It was held that the electronic signals sent by Bidders Edge to retrieve information from eBay’s system were sufficiently tangible to support a cause of action.⁹⁰ The court concluded that although the searches used only a small portion of eBay’s system capacity, Bidders Edge has nonetheless deprived eBay the ability to use that portion of its personal property for its own purposes.⁹¹

The court in *Oyster Software v. Forms Processing* disagreed that a showing of

⁸⁶ *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000); *eBay, Inc. v. Bidders Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D.Cal. 2000); Quilter, *supra* note 81, at 428-29.

⁸⁷ Warner, *supra* note 85, at 156.

⁸⁸ *eBay, Inc.*, 100 F. Supp. 2d at 1073.

⁸⁹ *Id.* at 1069-70.

⁹⁰ *Id.*

⁹¹ *eBay, Inc.*, 100 F. Supp. 2d at 1071.

interference of a computer system caused by a robot need be more than negligible.⁹² The outcome is not determined on whether the interference to plaintiff's system is substantial, but simply whether defendant's conduct amounted to use of plaintiff's computer.⁹³

In *Register.com v. Verio*, the District Court granted an injunction prohibiting Verio from utilizing software robots to access Register.com's WHOIS database and collect registrant information for use in mass marketing.⁹⁴ Verio was notified that its search robot was unwelcome on the Register.com site, thus any future use would constitute unauthorized access.⁹⁵ Register.com was particularly worried that the strain on their system caused by Verio's searches may result in its malfunction and crash.⁹⁶ Accordingly, if these unauthorized searches were to be deemed legal, it may induce other purveyors of internet based services to engage in similar conduct.⁹⁷

As with the CFAA, the focus of protection is not the information itself, but the medium on which it is stored. Damages are assessed only if they proximately resulted from the unauthorized access of the defendant.⁹⁸ Thus, in our Moviedex hypothetical, our entrepreneur will succeed under the trespass to chattels doctrine only through a showing of damages caused by the alleged infringer's access and copying. As the Oyster court stated, however, the interference does not have to be substantial.

⁹² *Oyster Software, Inc. v. Forms Processing, Inc.*, 2001 WL 1736382, *13 (N.D.Cal. 2001).

⁹³ *Id.*

⁹⁴ *Register.com, Inc.*, 126 F.Supp.2d at 255 .

⁹⁵ *Id.* at 249.

⁹⁶ *Id.* at 250.

⁹⁷ *Id.*

⁹⁸ *eBay, Inc.*, 100 F. Supp. 2d at 1069-70.

II. INTERNATIONAL ATTEMPTS TO CREATE A UNIFORM SYSTEM OF PROTECTION FOR DATA COMPILATIONS.

Through the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO), the international community has attempted to balance the interests of protecting owners of data compilations while promoting harmonization and uniformity of international law concerning intellectual property rights.⁹⁹

During the Uruguay round of the General Agreement on Tariffs and Trade (GATT), now administered by the World Trade Organization (WTO), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) was presented to promote effective and adequate protection of intellectual property rights and reduce impediments to international trade.¹⁰⁰ In order to achieve this goal, differences in national legal systems, pertaining to the enforcement of trade-related intellectual property rights, had to be accounted for.¹⁰¹ Accordingly, TRIPS was enacted to create a basis or standard of international protection for intellectual property rights.¹⁰² All members must give effect to the provisions of the agreement.¹⁰³ Additionally, members may implement laws more extensive than those required by the agreement as long as they do not conflict with the provisions of TRIPS.¹⁰⁴ Each member must accord the nationals of other members no less favorable treatment than it accords its own nationals pertaining to protection of

⁹⁹ See World Intellectual Property Organization: Copyright Treaty, Jan. 20, 1997, 36 I.L.M. 65; see also Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods, Apr. 15, 1994, 33 I.L.M. 81 [hereinafter TRIPS].

¹⁰⁰ TRIPS, *supra* note 99, at 84.

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.* at 84-85..

¹⁰⁴ TRIPS, *supra* note 99, at 85.

intellectual property rights.¹⁰⁵

TRIPS expressly incorporates the substantive requirements of the Berne Convention, thereby requiring member states to provide a minimum standard of protection to intellectual property rights under their respective national laws.¹⁰⁶ Thus, by incorporation, TRIPS includes 1) a set of minimum rights; 2) prohibition on formalities as a condition for enjoying rights; 3) retroactive protection for existing works in which copyright has not expired; 4) restrictions on the extent to which a member may limit protections; 5) a minimum term of protection for the life of the author plus fifty years; and 6) a national treatment provision.¹⁰⁷

The TRIPS agreement allows for protection of data compilations, but requires an originality component through selection or arrangement as to establish an intellectual creation.¹⁰⁸ Protection does not extend to the data or material itself.¹⁰⁹ As such, the standard is similar to that of United States copyright law and is consistent with the Supreme Court's decision in *Feist*.¹¹⁰

TRIPS establishes that a country may bring an action against another country through the WTO dispute resolution system.¹¹¹ If a TRIPS related infringement claim arises, a member of the WTO may request the establishment of a panel to settle the dispute.¹¹² The panel's decision

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 87; Freno, *supra* note 27, at 180.

¹⁰⁷ Freno, *supra* note 27, at 180.

¹⁰⁸ TRIPS, *supra* note 99, at 87.

¹⁰⁹ *Id.*; Amy Sullivan, *When the Creative is the Enemy of the True: Database Protection in the U.S. and Abroad*, 29 AIPLA Q.J. 317, 353 (2001).

¹¹⁰ Sullivan, *supra* note 109, at 353.

¹¹¹ World Trade Organization, *Understanding the WTO: Settling Disputes – A Unique Contribution*, available at http://www.wto.org/english/thewto_e/whatis_e/tif_e/displ_e.htm; Freno, *supra* note 27, at 181.

¹¹² World Trade Organization, *Understanding the WTO: Settling Disputes – A Unique Contribution*, available at http://www.wto.org/english/thewto_e/whatis_e/tif_e/displ_e.htm.

can be appealed to an appellate body.¹¹³ If it is determined that a member is not complying with its obligations, they must either immediately begin compliance with any and all obligations, provide equivalent trade concessions, or face potential trade sanctions from the complaining party equivalent to the obligations sought.¹¹⁴

Although TRIPS allows the WTO to impose trade sanctions against infringers of intellectual property rights, the originality requirement imposes no further protection than that offered by copyright. Thus, authors of non-creative databases remain vulnerable.

The World Intellectual Property Organization (WIPO) is a specialized agency of the United Nations dealing exclusively with intellectual property and technology related issues, including the current conundrum facing data compilations.¹¹⁵ Currently, there are nearly 180 member states of WIPO, including the United States, searching for a means to protect the information industry by providing satisfactory security to data compilers on a worldwide scale while taking into account the users of such information as well.¹¹⁶

WIPO is currently responsible for drafting and negotiating international agreements to facilitate worldwide uniformity and candidness when dealing with technological or intellectual property issues.¹¹⁷ The goal of the organization, pertaining to data compilations, is to create a consistent instrument protecting the interests of owners to perpetuate the further creation and

¹¹³ *Id.*

¹¹⁴ *Id.*

¹¹⁵ Freno, *supra* note 27, at 177.

¹¹⁶ WIPO, *Medium-Term Plan for WIPO Program Activities: Vision and Strategic Direction of WIPO*, available at http://www.wipo.int/about-wipo/en/index.html?wipo_content_frame=/about-wipo/en/dgo/pub487.htm.

¹¹⁷ WIPO, *Medium-Term Plan for WIPO Program Activities: Vision and Strategic Direction of WIPO*, available at http://www.wipo.int/about-wipo/en/index.html?wipo_content_frame=/about-wipo/en/dgo/pub487.htm.

progression of information technology.¹¹⁸ According to the WIPO Standing Committee on Copyright and Related Rights, meaningful intellectual property protection for databases is needed to promote innovation and investment in informational products.¹¹⁹ It would provide an incentive to disseminate a variety of new compilations, both electronic and memory based, which would benefit society as a whole, both socially and economically.¹²⁰ However, WIPO has thus far failed to provide such universal protection for data compilations, requiring members to rely on existing forms of protection, such as copyright.¹²¹

The Berne Convention, administered by WIPO, requires each member to recognize minimum standards of protection, in a sense harmonizing copyright law.¹²² Although relevant only to literary and artistic works, the Berne Convention established an international basis for the protection of authors and their works through a policy of moral rights and integrity.¹²³

The primary purpose of the Berne Convention is to promote and protect the international rights of authors.¹²⁴ For example, the right to national treatment in countries of the Union other than the country of origin,¹²⁵ the right to be free of formalities,¹²⁶ the exclusive right of

¹¹⁸ See *The Legal Protection of Databases, Report by the European Union to the Standing Committee on Copyright and Related Rights*, World Intellectual Property Organization, 8th Sess. (2002), available at http://www.wipo.int/documents/en/meetings/2002/sccr/doc/sccr_8_8.doc.

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ Sullivan, *supra* note 109, at 355.

¹²² Freno, *supra* note 27, at 177.

¹²³ Berne Convention for the Protection of Literary and Artistic Works, July 24, 1971, art. 6bis, 25 U.S.T. 1341, 828 U.N.T.S. 221 [hereinafter Berne Convention].

¹²⁴ Berne Convention, *supra* note 123, at art. 1.

¹²⁵ *Id.* at art. 5(1).

¹²⁶ *Id.* at art. 5(2).

authorizing adaptations,¹²⁷ and the public performance of their work whether it be musical¹²⁸ or artistic reproduction.¹²⁹

The Berne Convention doesn't expressly extend copyright coverage to data compilations.¹³⁰ Rather, the Berne Convention states that protection will not be extended to miscellaneous facts or news of the day.¹³¹ Therefore, it appears that the Berne Convention was not intended to protect the factual compilations fostered in today's modern society.¹³²

WIPO adopted a Copyright Treaty in 1996 that specifically addresses copyright protection in compilations, but attached an originality requirement leaving non-original collections vulnerable.¹³³ The sui generis proposal organized by WIPO failed to persuade the delegates at the conference and was thus tabled.¹³⁴ Speculation persists that the only reason the proposal was tabled was there was not enough time during the conference to work out the details.¹³⁵ However, with the exception of Europe, nearly every country objected to the protection proposed in the draft treaty.¹³⁶ The United States failed to support the treaty because

¹²⁷ *Id.* at art. 12.

¹²⁸ *Id.* at art. 11.

¹²⁹ *Id.* at art. 14.

¹³⁰ *Id.* at art. 2(5).

¹³¹ *Id.* at art. 2(8).

¹³² *See generally*, Berne Convention art. 2.

¹³³ World Intellectual Property Organization: Copyright Treaty, Jan. 20, 1997, 36 I.L.M. 69.

¹³⁴ Sullivan, *supra* note 109, at 355.

¹³⁵ Wesley L. Austin, *A Thoughtful and Practical Analysis of Database Protection Under Copyright Law, and a Critique of Sui Generis Protection*, 3 FALL J. TECH. L. & POL'Y 3, 70 (1997).

¹³⁶ *Id.* at 68.

they did not want the added pressure to enact sui generis protection.¹³⁷ Specifically, the Clinton administration refused to endorse the proposal after the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine expressed reservations that it would “seriously undermine the ability of researchers and educators to access and use scientific data, and would have a deleterious long term impact on our nation’s research capabilities.”¹³⁸ This proposal would have established sui generis database protection as the international norm.¹³⁹

As intellectual property continues to increase in global relevance, WIPO will be challenged with augmenting and further developing an intellectual property system in a way that is instrumental to social and economic development.¹⁴⁰ The means chosen to facilitate such an end could bind the information community, and all consumers thereof, to protection that favors compilers, rather than consumers, of information.

III. THE ANSWER TO THE DATA COMPILATION DILEMMA AS IMPELENTED BY THE EUROPEAN COMMUNITY.

A regional agreement adopted by the European Community has disrupted the harmony of intellectual property rights, specifically those protecting compilations of data, by extending protection to non-creative databases through a sui generis provision.¹⁴¹ Therefore, not only do compilations containing a creative spark qualify for copyright protection, non-creative databases

¹³⁷ *Id.* at 68-70.

¹³⁸ *Id.* at 70.

¹³⁹ Sullivan, *supra* note 109, at 355.

¹⁴⁰ Memorandum of Director General Kamil Idris, available at http://www.wipo.int/about-wipo/en/index.html?wipo_content_frame=/about-wipo/en/dgo/pub487.htm.

¹⁴¹ EU Directive 96/9, art. 7, 1996 O.J. (L 77) 3.

will receive protection if compiled through substantial labor or investment determined quantitatively and qualitatively.¹⁴²

The database directive was adopted in 1996 by the European Parliament to harmonize Community law and increase the protection of data compilations through a multi-tiered approach of copyright and a new, *sui generis* right.¹⁴³ All Member States are required to enact legislation to comply with the directive, thus creating a uniform system of data compilation protection within the European Community as of January 1998.¹⁴⁴

The directive provides for copyright protection for original databases that, by reason of selection or arrangement, demonstrate an author's own intellectual creation.¹⁴⁵ Therefore, the copyright protection is similar to that offered under U.S. copyright law, the WIPO Copyright Treaty, and TRIPS.¹⁴⁶

The directive further establishes a *sui generis* right of protection for non-creative databases, if a substantial investment has been made, measured either quantitatively or qualitatively, to obtain, verify, or present the contents so as to prevent extraction or duplication in whole or in part.¹⁴⁷ In effect, the *sui generis* provision creates a "sweat of the brow" doctrine whereby compilations are protected not based upon their creativity, but upon the effort, time, and

¹⁴² *Id.*

¹⁴³ *See Id.*

¹⁴⁴ EU Directive 96/9, *supra* note 141, at art. 16(1).

¹⁴⁵ *Id.* at art. 2(1).

¹⁴⁶ Jordan M. Blanke, *Vincent Van Gogh, "Sweat of the Brow," and Database Protection*, 39 AM. BUS. L.J. 645, 676 (2002).

¹⁴⁷ EU Directive 96/9, *supra* note 141, at art. 7(1).

expense that went into creation.¹⁴⁸

Although mandatory compliance was required of all Member States as of January 1998, 1999 found several members lacking such enactment legislation. Thereafter, the European Commission took matters into their own hands and sued the individual states for failure to comply with the directive. In 1999, the Commission of European Communities brought suit against Ireland in the European Court of Justice for failure to adopt laws, regulations or administrative provisions necessary to comply with the database directive.¹⁴⁹ A similar case was brought against the Grand Duchy of Luxembourg for failure to comply with the directive.¹⁵⁰

To protect database producers within the Community, the European Parliament included a strict reciprocity provision granting protection to non-members only if such third countries offer comparable protection to databases produced by nationals of a Member State or persons who have their habitual residence in the territory of the Community.¹⁵¹ In a sense, the Community adopted the stance of “we’ll scratch your back if you scratch ours.” Therefore, the only way to receive protection for data compilations vis-à-vis European Community nationals is for governments to provide reciprocal protection, in effect creating a de facto system of international sui generis rights.¹⁵² Otherwise, data compilers would have to reside in or designate their principle place of business within the Community formed in accordance with the

¹⁴⁸ See EU Directive art 7(1); Charles McManis, *Database Protection in the Digital Information Age*, 7 ROGER WILLIAMS U. L. REV. 7, 36 (2001).

¹⁴⁹ Case C-370/99, *Commission of the European Communities v. Ireland*, 2001 E.C.R. I-297 (2001).

¹⁵⁰ Case C-348/99, *Commission of the European Communities v. the Grand Duchy of Luxembourg*, 1999 O.J. C333/20 (1999).

¹⁵¹ EU Directive 96/9, *supra* note 141, at art. 11.

¹⁵² See EU Directive 96/6, Recital 56, 1996 O.J. (L 77) 6.

laws of the particular Member State to reap the benefit of the sui generis provision.¹⁵³

Since each Member State of the Community is required to enact laws to further the implementation of the directive, the courts of the individual states will be required to interpret and implement Community law.¹⁵⁴ The responsibility of interpretation of Community law will no longer fall strictly on the shoulders of the Justices of the European Court. The motivation for such a course of action is similar to the strategy of WIPO or the reasoning behind the enactment of the TRIPS agreement; to create a consistent, uniform law regionally, rather than globally, that favors conditions so Community Members may compete in the information market on a global scale.¹⁵⁵ Although relatively early in the interpretation and adjudication of the directive, the individual courts seem willing and able to dispense justice at the regional level to advance the interests of the Community.¹⁵⁶

In *British Horseracing Board Ltd. v. William Hill Organization*, the Court of Appeal (Civil Division) agreed with the ruling pronounced by the High Court of Chancery that data removed from a raw data feed, as part of the British Horseracing Board's (BHB) database, by Hill was an unlicensed extraction resulting in injunction.¹⁵⁷ Although the Appeals Court reversed the permanent injunction, it was not for improper interpretation of the directive by the trial judge.¹⁵⁸ Rather, it was due to other forms of remedy such as the licensing agreement

¹⁵³ EU Directive 96/9, *supra* note 141, at art. 11(1)-(2).

¹⁵⁴ *See* Blanke, *supra* note 146, at 677.

¹⁵⁵ *See* EU Directive 96/9 Recitals, 1996 O.J. (L 77).

¹⁵⁶ *See* Xuqiong Wu, *Foreign and International Law: Database Protection E.C. Database Directive*, 17 BERKELEY TECH. L.J. 571, 578 (2002).

¹⁵⁷ *British Horseracing Board v. William Hill Organization*, 2002 E.C.C. 24, 29 (2001).

¹⁵⁸ *British Horseracing Board*, 2002 E.C.C. at 48.

offered by BHB.¹⁵⁹ Furthermore, the court was worried about the differing opinions and interpretations of the directive handed down from other national courts within the Community.¹⁶⁰ The Court of Appeals believed that the European Court of Justice should decide a case if nothing more than to provide guidance towards interpretation to Union Members.¹⁶¹

The German Federal Supreme Court concluded that directories were considered databases, whether electronic or not, and protection could not be refused on the ground that they were official works.¹⁶² Although decided in the context of copyright under the directive, the court determined that the database did qualify for protection because it represented a substantial investment by the claimants.¹⁶³ Consequently, the producer of the database has a right to an injunction.¹⁶⁴

It is still early to tell the ramifications of the directive on the information and technology industry outside the European Community. However, many theories have been proffered that the rest of the world will fall in line with similar legislation, the EC will become the world leader in information technology, or the industry leaders, including the United States, will take a protectionist stance, thus obstruct the global diffusion of information.

Relating the *sui generis* right to our hypothetical, there is no doubt that our entrepreneur will have a cause of action for infringement against his competitor since he extracted the entire database without authorization for his own personal financial gain. The database was compiled

¹⁵⁹ *Id.*

¹⁶⁰ *Id.* at 46-48.

¹⁶¹ *Id.*

¹⁶² *Re the Unauthorized Reprod. of Telephone Directories on CD-Rom*, 2000 E.C.C. 433, 435 (1999).

¹⁶³ *Id.* at 438-39.

¹⁶⁴ *Id.* at 438.

through enormous effort and significant monetary expense, thus even though no protection exists under copyright, the sui generis provision protects the fruit of his labor. However, is this amount of protection desirable to society as a whole? Won't this sui generis provision effectively grant the author an exclusive right in the ideas and facts the database contains?

IV. HOW MUCH PROTECTION IS TOO MUCH?

The Supreme Court in *Feist* warned of the potential dangers of providing protection for so called “sweat of the brow” data compilations.¹⁶⁵ Specifically, Justice O'Connor worried that extending protection to data compilers solely on account of hard work and painstaking labor or a significant financial undertaking would lead to a virtual monopoly on ideas and facts.¹⁶⁶ Protection in the compilation would extend beyond mere selection and arrangement to the facts and ideas themselves.¹⁶⁷ Thus, any industrious individual could potentially throw together any number of compilations and effectively carve out for himself a corner of the information market.

Unfortunately for these budding entrepreneurs, facts and ideas do not owe their origin to any act of authorship.¹⁶⁸ No one can claim originality or ownership to facts or ideas because they were not actually created by the author, but merely discovered or reported.¹⁶⁹ Facts and ideas maintain their importance by remaining in the public domain, free for all to use and exploit, essentially to build upon the work and experiences of those who have gone before.¹⁷⁰

Consequently, this rationale establishes that protection for data compilers in the fruits of their

¹⁶⁵ *Feist*, 499 U.S. at 353.

¹⁶⁶ *Id.* at 354.

¹⁶⁷ *Id.* at 353.

¹⁶⁸ *Id.* at 347.

¹⁶⁹ *Id.*

¹⁷⁰ *Id.* at 349-50.

labors is thin.¹⁷¹

Although protection for owners of non-creative data compilations remains relatively weak in the United States, the alternative presented by the European Community could effectively stop the dissemination of information to the masses and have a detrimental effect upon society as a whole. Generally speaking, the American population is a well informed, educated group. This is, in part, due to the Freedom of Information Act¹⁷² and related privacy rights.¹⁷³ No firm or industry has a corner on the information technology market in the United States so as to impede the flow of information to the populace.

The sui generis right espoused by the Database Directive, however, protects owners of compilations if a showing of substantial investment is made.¹⁷⁴ Potentially, all databases could gain protection through such a provision if all that is required is the expenditure of labor or capital. The labor wouldn't necessarily have to be your own; you could pay someone else to do the work. The gist of the problem occurs, however, when subsequent authors want to use or market the same, or similar work, to that which has been compiled through cost or sweat.

Significantly, the European Court of Justice has yet to rule on a case interpreting the database directive.¹⁷⁵ In 2002, the English Court of Appeal (Civil Division) filed a reference for a preliminary ruling, but the pending decision remains unavailable.¹⁷⁶ The appeal in question,

¹⁷¹ *Fiest*, 499 U.S. at 349.

¹⁷² 5 U.S.C. § 552 (2000).

¹⁷³ U.S. CONST. amend XIV. (privacy rights are derived from the due process and equal protection clauses of the Fourteenth Amendment).

¹⁷⁴ *See* EU Directive 96/9, *supra* note 141, at art. 7.

¹⁷⁵ *British Horseracing Board v. Hill Organization*, 2002 E.E.C. 24, 471-472 (2001); European Court of Justice, available at <http://curia.eu.int/en/content/juris/index.htm>.

¹⁷⁶ *British Horseracing Board*, 2002 E.E.C. at 474.

British Horseracing Board v. Hill Organization, concerns the appropriateness of a permanent injunction imposed upon Hill for his dissemination of information received from the British Horseracing Board's (BHB) database.¹⁷⁷

BHB and their members compiled an electronic database of racing information at considerable cost to themselves.¹⁷⁸ The database is constantly updated with the latest information.¹⁷⁹ BHB charges a fee for the use of the information contained in the database, but this fee only recoups a third of what it costs to update and maintain.¹⁸⁰

Hill is a large bookmaker in the United Kingdom with valid licenses from BHB for certain information services related to his bookkeeping business.¹⁸¹ However, the service in question, the "raw data feed," was not licensed to Hill; rather he obtained this service through an independent company, Satellite Information Services (SIS), who had a valid license from BHB.¹⁸² SIS had no authority to sublicense BHB's information to Hill.¹⁸³ Hill would subsequently take that information and post it on his website for his customers to access.¹⁸⁴

The judge relied upon the recitals of the directive and reasoned that "infringement of the new right is not avoided by taking the contents and rearranging them and that what has to be protected is not primarily the form [of the database] but the investment which went into

¹⁷⁷ *See id.*

¹⁷⁸ *British Horseracing Board*, 2002 E.E.C. at 462.

¹⁷⁹ *Id.*

¹⁸⁰ *Id.* at 463.

¹⁸¹ *Id.* at 464.

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ *Id.*

obtaining, verifying and presenting the contents.”¹⁸⁵ The judge determined that the act of taking information from the raw data feed and transferring it to his website was extraction and making the site available to the public amounted to reutilization.¹⁸⁶

The court went on to discuss the time limits for protection under the sui generis provision. Although Article 10(1) grants protection for fifteen years after completion, Article 10(3) allows for reinstatement of the fifteen year limit if a substantial change, evaluated quantitatively or qualitatively, would result in the compilation being considered a substantially new investment.¹⁸⁷ Even if this change was nothing more than updating or the accumulation of successive additions.¹⁸⁸ Article 10(3), therefore, essentially allows data compilers to renew their fifteen year term of protection by updating and verifying the information contained therein, basically what amounts to nothing more than routine file maintenance.

The Court of Appeals reversed the permanent injunction imposed by the Court of High Chancery, but not because they determined Justice Laddie misinterpreted the law.¹⁸⁹ Rather, the court determined that the injunction was unnecessary because BHB had potential protection under a license.¹⁹⁰ Additionally, the court didn’t want to contribute to the conundrum of opinions handed down by other national courts if there was a potential for misinterpretation of the directive.¹⁹¹ Instead, a reference of questions was sent to the European Court of Justice.¹⁹²

¹⁸⁵ *British Horseracing Board*, 2002 E.E.C. at 468.

¹⁸⁶ *Id.* at 469.

¹⁸⁷ EU Directive 96/9, *supra* note 141, at art. 10; *British Horseracing Board*, 2002 E.E.C. at 469.

¹⁸⁸ *British Horseracing Board*, 2002 E.E.C. at 469.

¹⁸⁹ *Id.* at 474.

¹⁹⁰ *Id.*

¹⁹¹ *British Horseracing Board*, 2002 E.E.C. at 473.

Such a right to protect all “sweat of the brow” compilations could effectively cut off the free flow of information enjoyed by our historically open society by extending protection to compilers over facts and ideas. The Supreme Court’s opinion in *Feist*, however, has thus far prevented such an undesirable outcome.¹⁹³ If facts were protectable by the authors who published them, society as we know it today would not exist. The promotion of science and the useful arts, a constitutional mandate, would be rendered fruitless because subsequent authors would be unable to utilize works of their predecessors.

Science and technology, progress, is furthered by standing on the shoulders of those who came before us, not by starting from scratch. In fact, there are certain works that, if facts could be protected by authors, could never be created. Certain historical texts and biographies would not be composed because it would be virtually impossible to research and compile without infringing on a current author’s rights. For instance, a biography on the life of Louis XIV or a historical compilation of sixteenth century European warfare would be more or less impossible to create by independent means due to the historical context. Where else could you retrieve the needed information except from previous authors or sources written on the subject?

Although *sui generis* protection was implemented as an incentive to create new and improved data compilations, it is likely to have the opposite effect. Instead of encouraging authors, it may actually discourage them by potentially opening themselves up to liability if they copy information protected by another author. Future authors would be forced to pay a licensing fee to research protected information, then risk possible liability if the information researched is used commercially or otherwise outside the scope of the license. In this sense, the “sweat of the

¹⁹² *Id.* at 474.

¹⁹³ *See Feist v. Rural Telephone*, 499 U.S. 340 (1991).

brow” protection created by the sui generis right actually impedes the incentive to create.

Likewise, this provision conflicts with the constitutional mandate to “promote the progress of science and the useful arts.”¹⁹⁴ The protection of facts and ideas in data compilations would be counterproductive. It wouldn’t promote progress; rather it would hinder development of future works. It would require every author to start from scratch, recompile the information and facts, and still remain potentially liable for infringement. Future compilers would have to prove where and how they received the information they compiled to defend against accusatory inferences of misappropriation. Such proof would be the only defense against a claim of infringement. This would amount to an incredible waste of time, effort, and ingenuity.

Furthermore, since the originator of the compilation is under no obligation to provide access to his work at all, at minimal cost or otherwise, he could theoretically charge outrageous fees for such privilege. This control on the use of his work would impose significant costs on consumers.¹⁹⁵ After all, it is a matter of simple economics that if a single individual or entity controls access to data, the cost of such access will rise.¹⁹⁶

Another potential negative effect of universal sui generis protection of data compilations is that such information stoppage, or an increased cost to attain, may undermine the development of third world countries that depend upon the free flow of information from industrialized powers to jump start their economies. Today’s world economy will not wait for individual nations to catch up. Rather, the only way for many countries to compete economically is to adhere to the lessons of the industrial giants. If the information that led to the economic boom in

¹⁹⁴ U.S. CONST. art. I, § 8, cl. 8.

¹⁹⁵ Paul J. Heald, *The Extraction/Duplication Dichotomy: Constitutional Line-Drawing in the Database Debate*, 62 OHIO ST. L.J. 933, 941 (2001).

¹⁹⁶ *Id.*

the United States and Europe were to be suppressed, many third world countries would be at the mercy of the industrialized countries more than they already are.

**V. PROPOSED SOLUTION TO THE PROBLEM CONCERNING
PROTECTION OF NON-CREATIVE COMPILATIONS OF DATA.**

The protection established by the CFAA provides a much more sensible approach to the protection of information. Rather than protecting information itself, the CFAA provides for criminal and civil sanctions to deter the wrongful acts of information hackers.¹⁹⁷ The wrongful acts, however, are not based solely upon the misappropriation of information, but rather the unauthorized access, or abuse of access, to a protected computer.¹⁹⁸ For example, in *Register.com v. Verio*, the United States District Court for the Southern District of New York enjoined Verio from the further use of Register.com's WHOIS database due to excessive and unauthorized use of customer names and contact information for mass marketing purposes.¹⁹⁹

Register.com is a domain name registrar offering clients a host of services beyond registration of .com, .net, and .org domains.²⁰⁰ Besides services such as web site creation tools, web site hosting, and electronic mail, to name but a few, Register.com gives control to its customers concerning the receipt of commercial solicitations.²⁰¹ Customers are allowed to "opt-in" during the domain name registration process to receive sales and marketing communications from Register.com and private label partners.²⁰² However, to become an accredited domain

¹⁹⁷ See 18 U.S.C. § 1030 (2004).

¹⁹⁸ See 18 U.S.C. § 1030(a) (2004).

¹⁹⁹ See *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 255 (S.D.N.Y. 2000).

²⁰⁰ *Register.com, Inc.*, 126 F. Supp. 2d at 241.

²⁰¹ *Id.*

²⁰² *Register.com, Inc.*, 126 F. Supp. 2d at 241.

name registrar, you must enter into a registrar accreditation agreement with the Internet Corporation for Assigned Names and Numbers (ICANN).²⁰³ Under the accreditation agreement, domain name registrars are required to provide an online WHOIS database containing all names and contact information of all customers registered.²⁰⁴ The purpose of the WHOIS database is to provide necessary information in the event a domain name dispute occurs.²⁰⁵

Verio, with the aid of a search robot, accessed the WHOIS database of several domain name registrar's, including Register.com, and collected contact information for use in mass marketing.²⁰⁶ Although such contact information was to be accessible to the public, Register.com included conditions of use that prohibited third parties from using this information for mass marketing purposes.²⁰⁷

The District Court determined that Verio's access to the WHOIS database to obtain information for mass marketing purposes was unauthorized in violation of 18 U.S.C. § 1030(a)(2)(C).²⁰⁸ Likewise, the court found that the search robot employed by Verio to access Register.com's WHOIS database could cause physical damages exceeding five thousand dollars by impairing the availability of data or the availability of the system as a whole.²⁰⁹ Therefore, since physical damages are likely, in excess of the statutory amount, 18 U.S.C. § 1030(a)(5)(C)

²⁰³ *Id.*

²⁰⁴ *Id.*

²⁰⁵ *Id.*

²⁰⁶ *Id.* at 243.

²⁰⁷ *Id.* at 244.

²⁰⁸ *Id.* at 254.

²⁰⁹ *Id.* at 253.

is also implicated.²¹⁰

Similar situations may arise pertaining to the availability and access to information of former employees. In *EF Cultural Travel v. Explorica*, the First Circuit Court of Appeals determined that a former employee who accessed EF Cultural Travel’s website with the aid of a scraper program to pirate prices exceeded authorized access.²¹¹ Whatever authorization Explorica had to navigate around EF Cultural Travel’s website was exceeded by providing proprietary information and know-how to an internet consultant to facilitate the creation of a scraper program.²¹² The net effect of the unauthorized access was to undercut EF Cultural Travel in the touring industry.²¹³

The court reasoned that by use of the terms “damage or loss” in 18 U.S.C. § 1030(g), Congress anticipated recovery in cases involving other than purely physical damages.²¹⁴ Thus, the term loss would encompass a loss of goodwill, business, and the cost of diagnostic measures taken after such excessive or unauthorized access was discovered.²¹⁵ The diagnostic measures taken by EF Cultural Travel far exceeded the required five thousand dollar threshold, not to mention the potential loss of business and goodwill, therefore, the court affirmed the preliminary injunction against Explorica.²¹⁶

Furthermore, the First Circuit concluded that as we advance further into an increasingly

²¹⁰ *Register.com, Inc.*, 126 F. Supp. 2d at 253. 18 U.S.C. § 1030(a)(5)(C) has subsequently been amended by Pub.L. 107-56, Title VIII, § 814, Oct. 26, 2001, 115 Stat. 382.

²¹¹ *EF Cultural Travel*, 274 F.3d at 581.

²¹² *Id.* at 583.

²¹³ *Id.* at 580.

²¹⁴ *Id.* at 585.

²¹⁵ *Id.* at 584.

²¹⁶ *Id.* at 585.

electronic world, the occurrence of physical damage will reduce while the value of what has been stolen, from the victim's standpoint, and the increased security measures to make sure it doesn't recur will undoubtedly increase.²¹⁷ If the statute were interpreted to include only actual, physical damages, this would flout Congress' intent and leave the CFAA to languish in the twentieth century while violators move into the twenty-first and beyond.²¹⁸ However, the five thousand dollar threshold must still be met, whether the damages be actual or purely economic.²¹⁹

Although the European Parliament has deemed necessary the disproportionate protection of non-creative data compilations through the sui generis provision, a scheme similar to the CFAA could solve many potentially serious problems that may materialize further down the road. While the potential of running out of novel or revolutionary ideas seems preposterous, protecting the fruits of one's labors solely on account of significant expenditure of labor or capital will grant a proprietary interest in facts and ideas to the compiler. Eventually the ownership of facts and ideas could stymie the creation of novel or original products. Such an event would be detrimental to society as a whole.

One of the purposes mentioned for adoption of the database directive was economic conformity within the European Community.²²⁰ Such conformity could be wrought by less extensive means, however. The enactment of legislation similar to the CFAA could harmonize Community law in the same manner it applies to all jurisdictions within the United States. The European Parliament would enact the legislation thus requiring all Community Members to adopt laws and regulations in compliance therewith. Moreover, compliance will likely ensue

²¹⁷ *EF Cultural Travel*, 274 F.3d at 585.

²¹⁸ *Id.*

²¹⁹ *Id.*

²²⁰ *See* EU Directive 96/9, 1996 O.J. (L 77) 2-3.

faster because the issue of damages is less controversial than ownership and interpretation of the provision would be less complicated.

Protecting data compilations through an analysis of access and damages, rather than securing rights in the information itself, would leave the crucial facts and information where they belong, in the public domain accessible to everyone. Since facts and ideas themselves cannot be protected, they may be copied by others and reused. Thus any third party with an inkling to do so could create a substantially similar or exact copy of a database if done by legitimate means. The CFAA simply prohibits you from damaging the property of another or accessing information without, or in excess, of authorization.²²¹ The statute is based on a showing of damages, not what is protectable and what is not, as is the case under copyright, or a showing of significant investment, measured quantitatively or qualitatively, as the sui generis provision provides.²²² Hence, the conundrum of database protection would be simplified if analyzed under the rubric of the CFAA.

The ease in determining whether a violation has occurred would simplify the judiciary's task and the opinions delivered to justify it. The CFAA is a well written, straightforward statute that provides adequate protection for creative and non-creative databases alike. Yet it follows the constitutional mandate of our democratic society that information remain available for all those who would search for it, a free and open society.

Within the United States, many people have spoken with contention about increasing the protection of data compilations, however the proponents and business interests have the ear of

²²¹ See generally 18 U.S.C. § 1030(a) (2004).

²²² See 18 U.S.C. § 1030(a) (2004).

Congress, who seem to agree that protection for data compilation should be strengthened.²²³ The rationale is that a sui generis protection of our own would place us on even ground with the European Community and terminate the risk that compilation producers in the United States may take advantage of the European law and relocate within the Community. However, such a proposal to protect “sweat of the brow” compilations would effectively put smaller authors and compilers out of business. Likewise, it would deter future authors from compiling works for fear of infringement litigation.

The proponents of increased protection, especially database manufacturers, have spoken out in favor of implementing a similar guarantee to the sui generis approach taken by the European Community. They claim that the directive allows users to extract insubstantial parts of the content of the database, and is only tempered by the requirement that Member States prohibit the repeated systematic extraction or reutilization which conflict with the normal exploitation of the database.²²⁴ Furthermore, Member States are permitted to make exceptions for educational purposes or scientific research.²²⁵ This would assure data compilers who have invested significant time and effort into their product that it would be protected.

On the other hand, many opponents feel that increased data protection may stem the flow of information. A sui generis right would effectively destroy the public domain, leaving researchers and second comers at the mercy of compilation owners who may or may not grant licensing agreements.²²⁶ Likewise, compilation owners may deny third parties the right to use preexisting data in value-added applications, even when the third parties are willing to succumb

²²³ See *supra* pp. 5-8.

²²⁴ IAN C. BALLON, E-COMMERCE AND INTERNET LAW, chap. 9 § 9.04(3)(A) (2002).

²²⁵ *Id.*

²²⁶ BITS OF POWER: ISSUES IN GLOBAL ACCESS TO SCIENTIFIC DATA, box 5.4 (National Academy Press 1997).

to royalty-bearing licenses.²²⁷ Thus, the concept of incremental or cumulative and sequential innovation, which is central to the development of modern technological advancements, would be banished from the universe of database production, despite the economic waste and inefficiency inherent in such policies.²²⁸

The database manufacturing community may complain that protection must increase if we are to compete on the global market; the fact is, however, that the United States enjoys a sixty five to seventy percent share of the world market.²²⁹ If parasitical copying becomes a problem, Congress can legislate in response, but to institute an exclusive property right over information or an overly broad liability regime would produce equally undesirable social consequences.²³⁰ “Curing a putative risk of underprotection with a massive dose of overprotection of facts and data would severely compromise democratic discourse by limiting the ability of researchers, competitors, and the general public to build upon prior contributions to knowledge.”²³¹ The public benefits only when everyone has access to the building blocks of knowledge that may lead to creative and technological breakthroughs.²³²

Although many people, especially the information industry and their lobbyists, feel that adoption of a right similar or exact to the European Community’s sui generis right would perpetuate the uniformity needed to protect data compilations in today’s digital society, such a

²²⁷ BITS OF POWER, *supra* note 226.

²²⁸ *Id.*

²²⁹ *Statement Concerning H.R. 2652: Hearing Before the Subcommittee on Courts and Intellectual Property, 105th Cong. (1997)* [hereinafter *Hearing*] (statement of Professor J.H. Reichman) [hereinafter *Reichman Statement*] (Professor Reichman is a Visiting Professor of Law at the University of Michigan and a Professor of Law at Vanderbilt University).

²³⁰ *Id.*

²³¹ *Id.*

²³² *Id.*

course could also lead to a virtual monopoly of valuable information in the hands of a small segment of society. Rather, the more reasonable approach is to provide for criminal and civil sanctions for damages caused by individuals improperly accessing, or exceeding authorized access to, protected computers and databases. Further causes of action could be brought under the tort doctrine of Trespass to Chattels for programs or robots that invade the sovereignty of private servers. The concept to keep in mind, however, is that by using the CFAA and Trespass to Chattels, information is not necessarily being protected. Rather, sanctions are being imposed for the unauthorized access of the medium housing the information. Therefore, crucial information remains in the public domain free to be accessed at will by any and all who wish to use it, while fostering the constitutional plan of promoting the progress of science and the useful arts.